ELEMENTARY NUMBER THEORY

UZI VISHNE

ABSTRACT. Lecture Notes for "Elementary Number Theory", given as Math 180 at the first semester of 2002–3, Yale.

1. AXIOMS OF THE INTEGERS

Basic terminology of sets: if A is a set, $a \in A$ means that a belongs to A, and $a \notin A$ means that it is not. For two sets A, B, $A \subseteq B$ (A is contained in B) means that every element of A is also an element of B (but not necessarily vice versa).

The set of integers is denoted by

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Two operations are defined on $\mathbb{Z}$: addition and multiplication. They satisfy the following axioms.

$a + 0 = 0 + a = a$	neutral element for $+$
$\forall a \exists b \;\; a + b = 0$	inverse element for $+$
$a + b = b + a$	commutativity of $+$
$a + (b + c) = (a + b) + c$	associativity of $+$
$a \cdot 1 = 1 \cdot a = a$	neutral element for $\cdot$
$ab = ba$	commutativity of $\cdot$
$a(bc) = (ab)c$	associativity of $\cdot$
$a(b + c) = ab + ac$	distributivity of $\cdot$ with respect to $+$

Moreover, an order relation $\leq$ ("less than or equal to") is defined; it satisfies the following axioms:

For every a, b, either $a \leq b$ or $b \leq a$	linearity
$a \leq a$	reflexivity
$a \leq b$ **and** $b \leq a \implies a = b$	asymmetry
$a \leq b$ **and** $b \leq c \implies a \leq c$	transitivity
$a \leq b \implies a + c \leq b + c$	
$a \leq b$ **and** $0 \leq c \implies ac \leq bc$	

These 'trivial' axioms, and one further axiom (which will be presented later), are all we need in this course.

Date: July 4, 2005.

.

We can use the 'weak' order relation to define a 'strong' one:

Definition 1.1. *We say that $a < b$ (a is smaller than b) if $a \leq b$ but $a \neq b$. Otherwise (namely when $b \leq a$), we say that $a \not< b$.*

Proposition 1.2. *The relation '$<$' satisfies for every $a, b, c \in \mathbb{Z}$:*

$$\begin{array}{rll} a \not< a & & \text{irreflexivity} \\ a < b & \implies b \not< a & \text{antisymmetry} \\ a < b \ \textbf{and} \ b < c & \implies a < c & \text{transitivity} \end{array}$$

For simplicity, we may write $b \geq a$ instead of $a \leq b$ and $b > a$ instead of $a < b$. By definition, $\mathbb{N} = \{n \in \mathbb{Z} : n > 0\}$. This is the set of *natural numbers*.

Exercise 1.3. *Prove that the additive inverse (b such that $a + b = 0$) is unique.*

Solution. If $a + b_1 = a + b_2 = 0$, then

$$b_1 = b_1 + 0 = b_1 + (a + b_2) = (b_1 + a) + b_2 = 0 + b_2 = b_2.$$

□

Given $a \in \mathbb{Z}$, there is thus a unique number b such that $a + b = 0$, and we denote this number by $-a$.

Exercise 1.4. *Show that $-(-a) = a$.*

Solution. By definition $-(-a)$ is the number which when added to a gives 0; and indeed, $a + (-a) = 0$. □

Exercise 1.5. *Prove (from the axioms) that $0 \cdot a = 0$ for every $a \in \mathbb{Z}$.*

Solution. Let $b = 0 \cdot a$. Since $0+0 = 0$, we have that $b+b = 0 \cdot a+0 \cdot a = (0 + 0) \cdot a = 0 \cdot a = b$ so adding the additive inverse of b we find that $b = 0$. □

Exercise 1.6. *Prove (from the axioms) that $(-a)b = -(ab) = a(-b)$ and that $(-a)(-b) = ab$.*

Solution. $(-a)b = -ab$ since $(-a)b + ab = ((-a) + a)b = 0 \cdot b = 0$, and likewise $a(-b) = -ab$. Finally $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$. □

Exercise 1.7. *Prove (from the axioms) that $0 < 1$.*

Solution. Otherwise, we have from the linearity that $1 < 0$, and then (adding the additive inverse of 1 to both sides) we get that $0 < -1$. Multiplying by the (positive!) number -1, we find that $0 < (-1)(-1) = 1 \cdot 1 = 1$. □

2. Divisors

The fundamental concept of this section is the following:

Definition 2.1. *We say that $a|b$ (a divides b) if $b = ca$ for some integer c.*

Notice that we require c to be an integer; for every $a, b \in \mathbb{Z}$ ($a \neq 0$) there is a fraction ($r = \frac{b}{a}$) such that $b = ra$ — but this has nothing to do with a dividing b.

Example 2.2. $6|12$ *since* $12 = 2 \cdot 6$.

Proposition 2.3. *The division relation (on $\mathbb{N}$) is irreflexsive, anti-symmetric and transitive: for $a, b, c \in \mathbb{N}$,*

$$\begin{array}{rcl} a|a & & \textit{reflexivity} \\ a|b \textbf{ and } b|a & \Longrightarrow & a = b \quad \textit{asymmetry} \\ a|b \textbf{ and } b|c & \Longrightarrow & a|c \quad \textit{transitivity} \end{array}$$

Note that unlike the order relation, this relation is not linear; for example, none of the numbers $2, 5$ divide the other.

Proposition 2.4. *Basic properties of divisors: for every $a, b, c \in \mathbb{Z}$,*

1. $a|0$.
2. $1|a$.
3. *If $a|b$ then $a|bc$.*
4. *If $a|b$ then $ac|bc$.*
5. *If $a|b, c$ then $a|(b \pm c)$.*

Proof. 1. We have that $a|0$ since $0 = 0 \cdot a$.
2. Likewise, $1|a$ since $a = a \cdot 1$.
3. Follows from transitivity (since $b|bc$).
4. If $b = g \cdot a$ then $bc = g \cdot ac$.
5. If $b = g \cdot a$ and $c = h \cdot a$ then $b \pm c = (g \pm h) \cdot a$. □

Example 2.5. *The natural divisors of* 6 *are* $1, 2, 3, 6$. *The divisors of* 31 *are* $1, 31$. *The divisors of* 24 *are* $1, 2, 3, 4, 6, 8, 12, 24$.

One can draw a graph of the divisors of a number n, placing a below b iff $a|b$. Thus 1 is on the bottom, n on the top, and there are chains leading from 1 to n.

For every $a \in \mathbb{Z}$, we define $|a| = a$ if $a \geq 0$, and $|a| = -a$ otherwise.

Remark 2.6. *For every two integers a, b, $a|b$ iff $|a|$ divides $|b|$.*

3. Induction

If $A \subseteq \mathbb{Z}$ is a set, a minimal number of A is an element $a \in A$ such that $a \leq b$ for every $b \in A$. Not every set has a minimal element: for

example, $\mathbb{Z}$. An empty set cannot have a minimal element (it has no elements at all...).

Axiom 3.1 (Well ordering axiom)**.** *Every non-empty set of natural numbers has a minimal element.*

Sets of rational numbers not necessarily have minimum (like $A = \{r \in \mathbb{Q} : r > 0\}$, where for every $r \in A$, $r/2 \in A$ is smaller).

Exercise 3.2. *If $n \in \mathbb{N}$ then $n \geq 1$.*

Solution. By definition of $\mathbb{N}$, every $n \in \mathbb{N}$ satisfies $n > 0$. Suppose $n < 1$ for some $n \in \mathbb{N}$, and form the set $A = \{n, n^2, n^3, \dots\}$. Let b denote the minimum of this set, then $b = n^i$ for some $i = 1, 2, \dots$ (since these are the elements of A); now from $n < 1$ it follows that $bn < b$, but $bn = n^{i+1} \in A$, a contradiction to the minimality of b. □

An equivalent formulation is the induction principle, which follows from the axiom:

Corollary 3.3. *Let $P \subseteq \mathbb{N}$ be a set such that $1 \in P$, and for every n, if $n \in P$ then $n + 1 \in P$. Then $P = \mathbb{N}$.*

Proof. Otherwise let a be the smallest element outside P. Then $a \neq 1$ by assumption, so $a - 1 \in P$. But then $a \in P$, a contradiction. □

Let us prove some easy results using induction.

Example 3.4.

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2},$$
$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Example 3.5. *$n^3 - n$ is always divisible by 6.*

Proof. Check that $(n+1)^3 - (n+1) = (n^3 - n) + 3n(n+1)$. The result follows since $n(n+1)$ is always even. □

Example 3.6. *If n is odd, then $n^4 - 1$ is always divisible by 16.*

Proof. Put $n = 2m - 1$ and prove by induction on m. □

Here is a useful result proved by induction.

Proposition 3.7. *Every finite set has a maximal element.*

Proof. The set $A = \{a_1\}$ evidently has a_1 as maximum. Assume the claim holds for sets of $n - 1$ elements (where $n > 1$), and let $A = \{a_1, \dots, a_n\}$. Let a_i denote the maximal element of $\{a_1, \dots, a_{n-1}\}$ (which exists by the induction hypothesis). If $a_n > b$ then $a_n = \max A$, otherwise $a_i = \max A$. □

Form IP-1a: Proof by Induction

Claim: The statement _____ holds for every natural n.
Proof: The statement holds for $n = 1$: _____.
Assuming the statement holds for $n - 1$ [(1)(2)], one can prove it for n. Indeed: _____
_____
_____
_____
_____. □

(1) or even for any $1 \leq m < n$.

(2) this assumption is called 'the induction hypothesis'

By the power vested in this form by the Principle of Induction,

the statement is hereby declared valid.

FIGURE 1. Form IP-1a

The following is a stronger version of the Induction Principle (as it proves the same result $P = \mathbb{N}$ from weaker assumptions); it is useful for proofs by induction on divisors.

Theorem 3.8 (Generalized Induction Principle)**.** *If a property holds for* 1*, and for every* n*, from the fact that it holds for* $1, \ldots, n-1$ *it follows that it also holds for* n*, then the property holds for all numbers.*

Figure 1 gives the general shape of a proof by induction.

3.1. Factorization into primes - existence.

Definition 3.9. *A natural number* $p > 1$ *is called a prime if its only natural divisors are* $1, p$*.*

Example 3.10. *The primes below* 100 *are:*

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$

Theorem 3.11. *Every natural number* $n > 1$ *is divisible by some prime.*

Proof. By induction. The statement holds for $n = 2$ (since this is a prime). Assume it holds for $2, \ldots, n-1$. If n is prime, we are done. Otherwise it has a divisor $d < n$; but then $p|d$ for some prime p by induction, and $p|n$. □

The following important result is a direct corollary:

Theorem 3.12. *There are infinitely many primes.*

Proof. Otherwise, let $p_1, \ldots, p_t$ be the primes, and let $N = p_1 \ldots p_t + 1$. None of the primes divides N, contradicting Theorem 3.11. □

Theorem 3.13. *Every natural number $n > 1$ can be written as a product of primes.*

Proof. Induction on n: for $n = 2$ this is obvious. Assume the result holds for $2, \ldots, n-1$. If n is a prime, we are done. Otherwise, $n = ab$ — but then write $a = p_1 \ldots p_m$ and $b = p_{m+1} \ldots p_t$, and $n = p_1 \ldots p_t$. □

Example 3.14. $98160 = 2^3 \cdot 3 \cdot 10 \cdot 409$.

We will learn how to recognize primes and how to factorize numbers later in the course.

4. The greatest common divisor

4.1. **Definition.** The maximal divisor of a number $a \in \mathbb{N}$ is, of course, a. We define a similar notion for pairs of numbers.

Definition 4.1. *Let $a, b \in \mathbb{Z}$, not both zero.*

The greatest common divisor (a, b) of a, b is the largest number which divides both a and b.

If $a = b = 0$ then every number divides a, b, so we do not define $(0, 0)$.

Remark 4.2. *1. This definition uses Proposition 3.7.*

2. For every divisor $d|a, b$, $|d|$ is also a divisor (Remark 2.6). But after all $d \leq |d|$, so the greatest common divisor is always positive.

Proposition 4.3 (Basic Properties)**.**

1. For every $a, b \in \mathbb{Z}$,

$$(b, a) = (a, b).$$

2. Assume $a, b \in \mathbb{N}$. Then $(a, b) \leq \min\{a, b\}$.

3. If $a|a'$ and $b|b'$, then $(a, b)|(a', b')$ (since every divisor of a, b also divides a', b').

If $d = (a, b)$, then $d|a$ and we can write $a = da'$ for some integer $a' \in \mathbb{Z}$; likewise we can write $b = db'$. Concerning a', b', we have the following theorem:

Theorem 4.4. *Let $d = (a, b)$, and write $a = da'$ and $b = db'$. Then $(a', b') = 1$.*

Proof. For if $e|a', b'$, we have that $a' = ea''$ and $b' = eb''$, so that $de|a, b$; but then $de \leq d$ so that $e \leq 1$. □

Exercise 4.5. *For every n, $(n^2+1, n+1)$ is either 1 or 2.*

Solution. Suppose $d|n^2+1, n+1$. Then $d|(n^2-1) = (n+1)(n-1)$, and also the difference $2 = (n^2+1) - (n^2-1)$. □

4.2. **Application: the square root of 2.**

Definition 4.6. *We say that two natural numbers are co-prime if they have no common divisor larger than 1.*

Example 4.7. $15, 22$ *are co-prime.* $36, 16$ *are not (since both are divisible by 2). Likewise* $2, 0$ *are not co-prime (again, both are divisible by 2).*

The real numbers can be defined in a rigorous way using the integers, but this is outside the scope of this course. For us, the reals can be thought of as describing lengths of segments (where a unit segment is fixed), and indeed this was the approach taken by the ancient Greeks.

Definition 4.8. *A rational number is a (real) number of the form a/b, where $a, b \in \mathbb{Z}$, $b \neq 0$.*

We say that a rational number a/b is in reduced form, if $(a, b) = 1$.

Corollary 4.9. *A rational number a/b always have a reduced form.*

Proof. Let $d = (a, b)$, then $a/b = (a/d)/(b/d)$ and $a/d, b/d$ are co-prime by Theorem 4.4. □

Proposition 4.10. *There is no rational number which is the square root of 2.*

Proof. First note that the square of an even number is even, and the square of an odd number is odd (why?).

Assume $(a/b)^2 = 2$ where a, b are co-prime. Then $a^2 = 2b^2$, so a^2 and thus a is even. Write $a = 2a_1$, then $2a_1^2 = b^2$ so b^2 and thus b is even, contradicting the co-primeness assumption. □

4.3. **Factorization into primes - uniqueness.**

Proposition 4.11 (Division with residue)**.** *Fix $b > 0$. For every $n \geq 0$ we can write $n = qb + r$ for $0 \leq r < b$.*

Proof. If $b = 1$ the result is obvious, so assume $b > 1$.

For $n = 0$ the claim obviously holds ($0 = 0 \cdot b + 0$).

Assume it holds for n; if $b|n$, then $n = qb$ and $(n+1) = qb + 1$ where $0 < 1 < b$. Otherwise $n = qb + r$ for $r < b$. If $r < b - 1$, then $(n+1) = qb + (r+1)$ and still $0 < r+1 < b$. Otherwise $n = qb + (b-1)$ so that $n + 1 = qb + b = (q+1)b$. □

Remark 4.12. *The expression $n = qb + r$ with $0 \leq r < b$ is unique: for if $n = q'b + r'$ with $r' > r$, then $0 < r' - r < b$ is divisible by b, which is absurd.*

Corollary 4.13. *Suppose that $n = qb + r$. Then $b|n$ iff $r = 0$.*

Remark 4.14. *(a, b) divides any integer combination $\alpha a + \beta b$ of a, b.*

Example 4.15. *Write* 3 *as an integer combination of* $15, 24$.

Write 1 *as a combination of* 12 *and* 17*: (compare the lists*

$$12, 24, 36, 48, 60, 72, 84, \dots$$

$$17, 34, 51, 68, 85, 102, \dots)$$

Theorem 4.16. *Let $a, b > 0$. There are u, v such that $(a, b) = ua + vb$.*

Proof. Let $A = \{ga + hb : g, h \in \mathbb{Z}\} \cap \mathbb{N}$. The set is not empty as $a \in A$. Let e denote the minimal number in this set, and write $e = ua + vb$; also let $d = (a, b)$.

We obviously have that $d|e$ (Remark 4.14).

Suppose that e does not divide a. write $a = qe + r = q(ua + vb) + r$ for $0 < r < e$. Then $r = (1 - qu)a - vb \in A$, a contradiction to the minimality of e. So e divides a, and similarly it must divide b. But then $e \leq d$ and we have that $d = e$. □

Proposition 4.17. *If $a|bc$ and $(a, c) = 1$, then $a|b$.*

Proof. Write $1 = \alpha a + \gamma c$. Then we have that $b = (\gamma c + \alpha a)b = \gamma(bc) + \alpha ab$ and both summands are divisible by a. □

Example 4.18. 13 *divides* 1456000*, so it must divide* 1456.

Corollary 4.19. *If a prime p divides a product, then it must divide one of the factors.*

Proof. If p does not divide a, then $(p, a) = 1$. Assume $p|ab$. If p is co-prime to a, then by the proposition it divides b. □

Challange. Try to prove Proposition 4.17 or Proposition 4.19 without using Theorem 4.16.

Theorem 4.20 (Fundamental Theorem of Arithmetic)**.** *Every natural number $n > 1$ can be written in a unique way as a product of primes.*

Proof. Every number can be written as a product of primes by Theorem 3.13. We prove the uniqueness of such expressions by induction on n; for $n = 2$ the statement is clear. Assume $p_1 p_2 \dots p_s = q_1 \dots q_m$; then p_s divides (and thus equal to) one of the primes $q_1, \dots, q_m$ – reordering we may assume $p_s = q_m$. Cancelling them, the resulting two factorizations are equal up to reordering by the induction hypothesis. □

4.4. **More on the greatest common divisor.** The greatest common divisor is not only greater than every other common divisor, but also divisible by them:

Proposition 4.21. *If $e|a, b$, then $e|(a, b)$.*

Proof. Write $(a, b) = \alpha a + \beta b$, then since $e|a, b$ it also divides (a, b). □

Proposition 4.22. *For every a, b, k we have that $(ak, bk) = (a, b)k$.*

Proof. Let $d = (a, b)$. Since $d|a, b$, we have that $dk|ak, bk$. Now write $d = ua + vb$, then $dk = u(ak) + v(bk)$ so $(ak, bk)|dk$. □

Proposition 4.23. *For every n, a, b we have that $(n, ab)|(n, a)(n, b)$.*

Proof. Write $\alpha a + \beta n = (n, a)$ and $\alpha' b + \beta' n = (n, b)$, then $(n, a)(n, b) = (\alpha a + \beta n)(\alpha' b + \beta' n) = \alpha\alpha' ab + (\alpha a\beta' + \alpha' b\beta + \beta\beta' n)n$ which is a combination of ab, n, and thus divisible by (n, ab). □

Corollary 4.24. *If $(n, b) = 1$ then $(n, ab) = (n, a)$.*

Proof. Obviously $(n, a)|(n, ab)$ (see Remark 4.3.3). By the previous proposition we have $(n, ab)|(n, a)$, so we are done. □

Corollary 4.25. *If $(n, a) = (n, b) = 1$ then $(n, ab) = 1$.*

Proof. Special case of 4.24. □

In a slightly different direction, we can prove a refinement of Proposition 4.23. We first need another useful remark:

Remark 4.26. *Assume $(a, b) = 1$. If $a|n$ and $b|n$, then $ab|n$.*

Proof. Writing $n = an'$ we see that $b|an'$, but b is prime to a so by Proposition 4.17 $b|n'$ and $ab|an' = n$. □

Proposition 4.27. *If $(a, b) = 1$, then $(n, ab) = (n, a)(n, b)$.*

Proof. Write $c = (n, a)$ and $d = (n, b)$, and notice that since $c|a$ and $d|b$, we have that $(c, d)|(a, b) = 1$. From the last remark it then follows that $cd|n$.

Now write $a = ca'$ and $b = db'$, then $(n/c, a') = (n/d, b') = 1$ (Theorem 4.4), and $(n, ab) = cd(n/(cd), a'b')$, but $(n/(cd), a') = (n/(cd), b') = 1$ (as $n/c, a' = (n/d, b') = 1$), so we are done by Corollary 4.25. □

Proposition 4.28. *If $a|n$, then $(a, b) = (a, (n, b))$.*

Proof. Let $e = (a, b)$. Write $a = a'e$ and $b = b'e$, so that $(a', b') = 1$.

We have that $n = ak = a'ek$ for some k, and $(a, (n, b)) = (a'e, (a'ek, b'e)) = (a'e, e(a'k, b')) = e(a', (a'k, b'))$, but $(a', (a'k, b'))|(a', b') = 1$, so $(a, (n, b)) = e = (a, b)$. □

Proposition 4.29. *We have that* $((a,n),b) = (a,(n,b))$.

Proof. By Proposition 4.28,

$$((a,n),b) = ((a,n),(n,b)) = (a,(n,b)).$$

□

This was the elegant proof. But Theorem 4.20 is so powerful, that it can be used to prove this type of claims by brute force.

Proposition 4.30. *Write* n, m *using a common basis of primes:* $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ *and* $m = p_1^{\beta_1} \dots p_t^{\beta_t}$, *where* $\alpha_i, \beta_i \geq 0$.

a. We have that $n \mid m$ *iff* $\alpha_i \leq \beta_i$ *for every* i.

b. The g.c.d is $(n,m) = p_1^{\min(\alpha_i,\beta_i)} \dots p_t^{\min(\alpha_t,\beta_t)}$.

This can be used to prove all the results given above. For example, Proposition 4.23 translates to $\min(n, a+b) \leq \min(n,a) + \min(n,b)$.

5. Short Introduction to Complexity theory

Complexity theory deals with the time it takes an algorithm to complete its mission. We count 'basic operations', which could be addition and multiplication of decimal or binary digits, or more complicated operations like multiplication of two residues modulo a fixed number n.

The typical question in analyzing an algorithm is how many steps it will require, depending on the size of the input. For example, it will take at most $n^2/2$ to sort n numbers in an iterative 'search the minimum' method; but there are better methods, which will only require about $n\log(n)$ steps. Since the basic operation is not determined (and in any case it depends on the application of the algorithm, which from a theoretical point of view is not so interesting), we are not concerned with constant multiples of the complexity: thus an algorithm taking $3n\log(n)$ steps is about as good as the one taking $n\log(n)$ steps, and they are both better than one taking $n^2/2$ (or $n^2/100$) steps.

If $f(n)$ is a function (such as n^2 or $n\log(n)$), we use the notation $O(f(n))$ to denote a complexity of the order of f, meaning any constant multiple of $f(n)$.

Another important convention is that we are concerned with the worst case scenario. For example it will only take $O(n)$ comparisons to recognize that a given list $a_1, \dots, a_n$ is already ordered, but we do not assume that this will be the case in general.

Notice that in a number-theoretic problem, where the input are numbers (of size roughly n, say), the size of the input is $\log(n)$ (for this is the number of digits required to describe n). An algorithm with

complexity $O(\log(n)^k)$ (for a fixed k) is thus called *polynomial*, while algorithms of complexity n^a ($a > 0$) are *exponential*.

Obviously, even the basic operations depend on the size of the numbers involved. In fact, it takes about $\log(n)$ basic (digital) operations to add two numbers of the size of n, and multiplication takes $\log(n)^2$ decimal operations. Division and taking a number m (with $O(\log(n))$ digits) modulo n take about $\log(n)^3$ operations.

The logarithms mentioned so far are to base 10. However, recall that $\log_{10}(n) = \log_{10}(2) \cdot \log_2(n)$, so the number of basic operations only change by a constant if we consider binary operations rather than decimal ones.

In the algorithms that follow, we usually compute the complexity in terms of basic operations modulo n. If the number of basic steps is polynomial, the same will hold for the number of operations on digits, and the algorithm will rightfully be said to be polynomial.

6. Euclid's algorithm

6.1. **The basic algorithm.** The purpose of this subsection is to present an efficient algorithm to compute (a, b). Indeed, Proposition 4.30 gives a formula for this quantity — but it depends on a decomposition of a, b into prime factors, and in general this is a difficult task.

We start with the following observation:

Proposition 6.1. *If $a = qb + r$, then $(a, b) = (b, r)$.*

Proof. Given that d divides b it obviously divides a iff it divides $r = a - qb$. □

Algorithm 6.2. *Given a, b, we wish to compute $d = (a, b)$.*

1. *If $a < 0$, set $a = -a$. If $b < 0$, set $b = -b$. If $a < b$, switch a, b. If $a = b = 0$, exit (illegal input).*
2. *Set $a_0 = a$ and $b_0 = b$.*
3. *Set $n = 0$ (for a start).*
4. *If $b_n = 0$, then $d = a_n$ and we are done.*
5. *Write $a_n = q_n b_n + r_n$ such that $0 \leq r_n < b_n$.*
6. *Set $a_{n+1} = b_n$ and $b_{n+1} = r_n$.*
7. *Advance n (to $n + 1$).*
8. *Return to step 4.*

Example 6.3. *Suppose $a = 17$ and $b = 12$. Then we have*

$n=0 \quad a_0=17 \quad b_0=12 \quad q_0=1 \quad r_0=5$
$n=1 \quad a_1=12 \quad b_1=5 \quad q_1=2 \quad r_1=2$
$n=2 \quad a_2=5 \quad b_2=2 \quad q_2=2 \quad r_2=1$
$n=3 \quad a_3=2 \quad b_3=1 \quad q_3=2 \quad r_3=0$
$n=4 \quad a_4=1 \quad b_4=0$
so the algorithm ends in step $n=4$, and returns $d=a_4=1$.

Proposition 6.4. *Algorithm 6.2 works (i.e. returns the greatest common divisor).*

Proof. We need to prove that the algorithm ends with $d=(a,b)$. The proof is by induction on b. If $b=0$, the algorithm stops in step 4 and returns $d=a$, which is the correct answer.

Assume the algorithm is correct for pairs (a,b') for every $b'<b$; then, given a,b, the second cycle starts with b,r_0 where $r_0=a-q_0b$ and $0\leq r_0<b$, so by the induction hypothesis it will return $d=(b,a-q_0b)$; but we already know that $(b,a-q_0b)=(a,b)$. □

For the complexity analysis of the algorithm, we need the following.

Definition 6.5. *The Fibonacci sequence is defined by*

$$F_0=F_1=1, \qquad F_{n+1}=F_n+F_{n-1}.$$

Proposition 6.6. *Let $\omega=\frac{\sqrt{5}+1}{2}$ and $\bar{\omega}=\frac{1-\sqrt{5}}{2}$. Then*

$$F_n=\frac{1}{\sqrt{5}}(\omega^{n+1}-\bar{\omega}^{n+1}).$$

Proof. We first note that $\omega^2=\omega+1$ and $\bar{\omega}^2=\bar{\omega}+1$. Let $f_n=\frac{1}{\sqrt{5}}(\omega^{n+1}-\bar{\omega}^{n+1})$, and notice that $f_{n+1}=f_n+f_{n-1}$.

By induction. We have that

$$f_0=\frac{1}{\sqrt{5}}(\omega-\bar{\omega})=\frac{\sqrt{5}}{\sqrt{5}}=1,$$

and

$$f_1=\frac{1}{\sqrt{5}}(\omega^2-\bar{\omega}^2)=\frac{1}{\sqrt{5}}(\omega-\bar{\omega})=1.$$

The result then follows by induction. □

Remark 6.7. *Notice that $|\bar{\omega}|<1$, so that $\bar{\omega}^n\longrightarrow 0$ and $F_n\sim\omega^{n+1}/\sqrt{5}$.*

Theorem 6.8. *If $0\leq a,b\leq F_m$ where $m\geq 1$, then Algorithm 6.2 computes (a,b) in no more than m steps.*

Proof. By induction on m. If $m=1$ then $0\leq a,b\leq 1$ which forces the pairs $(1,1)$ or $(1,0)$ (recall that $(0,0)$ is undefined). The algorithm ends at step 1 in the first case, and step 0 in the second.

Suppose the claim is true for all pairs $a, b \leq F_{m'}$ when $m' = m - 1, m - 2$, and assume $a, b \leq F_m$. The algorithm starts with $a_0 = a$ and $b_0 = b$; writing $a_0 = q_0 b_0 + r_0$, we then set $a_1 = b_0 = b$ and $b_1 = r_0$. If $b \leq F_{m-1}$, then by the induction hypothesis it will take the algorithm no more than $m-1$ steps to complete from this pair, making it m steps together with the first one. So assume $b > F_{m-1}$, then, since $a \geq b$, we have that $q_0 \geq 1$ and $r_0 = a_0 - q_0 b_0 \leq a_0 - b_0 < F_m - F_{m-1} = F_{m-2}$; so the algorithm requires no more than $m-2$ steps from $a_2 = r_0, b_2$ to complete. □

Corollary 6.9. *Assume $a > b > 0$, then the algorithm requires no more than $\log_\omega a + 1/2$ steps to compute (a, b).*

Proof. Let m be the minimal number such that $a \leq F_m$ (so that $F_{m-1} < a$). By the theorem, the algorithm computes (a, b) in no more than m steps. But $a \geq F_{m-1} + 1 > \omega^m/\sqrt{5}$, and $m < \frac{\log(\sqrt{5})+\log(a)}{\log(\omega)} < \log_\omega(a) + 1/2$. □

This corollary bounds the number of steps required to compute (a, b) as logarithmic in $\max(a, b)$. Notice that it is in fact also logarithmic in $\min(a, b)$ (as the smaller number becomes a_1 after only one step).

6.2. **Extended Euclid's algorithm.** The generalized version of the Euclidean algorithm requires some manipulation of vectors and 2×2 matrices over $\mathbb{Z}$. We need to know the following facts:

Definition 6.10. *A 2×2 matrix over $\mathbb{Z}$ is an array of four integers, arranged in a square formation. A column vector is an array of two numbers, one over the other.*

The special matrices and operations are defined as follows:

Definition 6.11.

$$\vec{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Definition 6.12. *By definition*

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} v_1 + w_1 \\ v_2 + w_2 \end{pmatrix},$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix},$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} a_{11} v_1 + a_{12} v_2 \\ a_{21} v_1 + a_{22} v_2 \end{pmatrix},$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix}.$$

Exercise 6.13. *Prove that for every two vectors u, v, w, we have that $u+v = v+u$ and $u+(v+w) = (u+v)+w$, and $\vec{0}+u = u+\vec{0} = u$. Also, there exist a vector x such that $u+x = x+u = \vec{0}$.*

Exercise 6.14. *Prove that for every two matrices A, B, C, we have that $A+B = B+A$ and $A+(B+C) = (A+B)+C$, and $0+A = A+0 = A$. Also, there exist a matrix D such that $A+D = D+A = \vec{0}$.*

Exercise 6.15. *Prove that for every matrices A, B, C and vectors v, w, we have that $A(B+C) = AB+AC$, $A(v+w) = Av+Aw$, $(A+B)v = Av+Bv$.*

Exercise 6.16. *For every matrices A, B, C and vector v,*

$$(AB)v = A(Bv)$$

and

$$(AB)C = A(BC).$$

With this new notation, we can now describe the extended algorithm.

Algorithm 6.17. *Given $a, b \in \mathbb{Z}$, we compute α, β, d such that $\alpha a + \beta b = d$ and $d = (a, b)$.*

1. *If $a < 0$, set $a = -a$. If $b < 0$, set $b = -b$. If $a < b$, switch a, b. If $a = b = 0$, exit (illegal input).*
2. *Set $a_0 = a$ and $b_0 = b$, and $A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $A_{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.*
3. *Set $n = 0$ (for a start).*
4. *If $b_n = 0$, then $d = a_n$, and α, β form the second row of A_{n-1}.*
5. *Write $a_n = q_n b_n + r_n$ such that $0 \le r_n < b_n$.*
6. *Set $a_{n+1} = b_n$ and $b_{n+1} = r_n$, and $A_{n+1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} A_n$.*
7. *Advance n.*
8. *Return to step 4.*

Example 6.18. *Suppose $a = 17$ and $b = 12$. Then we have*

```
int gcdWithCoefs(int a, int b, int *x, int *y) {
  /* Returns x,y such that x*a+y*b=gcd(a, b) */

  if (b == 0) {
    *x = 1;
    *y = 0;
    return (a);
  }
  else {
    int x1,y1,g;

    g = gcdWithCoefs(b, a%b, &x1, &y1);
    *x = y1;
    *y = x1 - y1 * (a/b);
    return (g);
  }
}
```

FIGURE 2. Extended Euclid's algorithm as a C function

n	a_n	b_n	q_n	r_n	A_n
0	17	12	1	5	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
1	12	5	2	2	$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot A_0 = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$
2	5	2	2	1	$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot A_1 = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix}$
3	2	1	2	0	$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot A_2 = \begin{pmatrix} -2 & 3 \\ 5 & -7 \end{pmatrix}$
4	1	0			

so the algorithm ends in step $n = 4$, and returns $d = a_4 = 1$; moreover,

$$(5) \cdot 17 + (-7) \cdot 12 = 1.$$

Proposition 6.19. *Algorithm 6.17 works.*

Proof. If $b = 0$ then the algorithm stops with $n = 0$, and the second row $(\alpha, \beta) = (1, 0)$ of A_{-1} satisfies $\alpha a + \beta b = a = (a, 0)$. Assume $b > 0$.

We claim that $\begin{pmatrix} a_k \\ b_k \end{pmatrix} = A_k \begin{pmatrix} a \\ b \end{pmatrix}$ for $k = 0, \ldots, n$. Indeed, for $k = 0$ this holds by definition of A_0 (and $a_0 = a$, $b_0 = b$). Assume the

claim holds for some k, then

$$\begin{aligned}
\begin{pmatrix} a_{k+1} \\ b_{k+1} \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \begin{pmatrix} a_k \\ b_k \end{pmatrix} && \text{by def. of } a_{k+1}, b_{k+1} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} A_k \begin{pmatrix} a \\ b \end{pmatrix} && \text{by the induction hypothesis} \\
&= A_{k+1} \begin{pmatrix} a \\ b \end{pmatrix} && \text{by definition of } A_{k+1}.
\end{aligned}$$

The algorithm ends with $b_n = 0$ and then outputs a_n; since this part is identical with Algorithm 6.2, we find that $\begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$ for $d = (a, b)$, and by the last claim $\begin{pmatrix} a_{n-1} \\ d \end{pmatrix} = \begin{pmatrix} a_{n-1} \\ b_{n-1} \end{pmatrix} = A_{n-1} \begin{pmatrix} a \\ b \end{pmatrix}$. It follows that $d = \alpha a + \beta b$ where (α, β) is the second row of A_{n-1}. □

Notice that the algorithm takes the same number of steps as Algorithm 6.2 (though each step is slightly more complicated).

7. Computations modulo n

Fix a natural number n. Recall Proposition 4.11, that every number can be written as $qn + r$, where $0 \leq r < n$. It turns out that we can define reasonable operations of addition and multiplication on the set of residues.

Definition 7.1. *We say that* $a \equiv b \pmod{n}$ *(a is equivalent to b modulo n) if* $n|(a - b)$.

Proposition 7.2. *The relation 'equivalent modulo n' satisfies the following properties:*

$$\begin{aligned}
a \equiv a \pmod{n} \qquad & \textit{reflexivity} \\
a \equiv b \iff b \equiv a \qquad & \textit{symmetry} \\
a \leq b \ \textbf{and} \ b \leq c \implies a \leq c \qquad & \textit{transitivity}
\end{aligned}$$

Proof. $a \equiv a$ since $n|0 = a - a$. If $a \equiv b$ then $n|(a - b)$, so $n|(b - a)$ and $b \equiv a$. Finally if $n|(a - b)$ and $n|(b - c)$ then $n|(a - b) + (b - c) = (a - c)$. □

Proposition 7.3. *If* $a \equiv a'$ *and* $b \equiv b'$, *then* $a + b \equiv a' + b'$ *and* $ab \equiv a'b'$.

It follows that the residue of $a + b$ or ab modulo n depends only on the residues of a, b (and not on a, b themselves).

Remark 7.4. *If for some* a, b, c, n *we have* $a \equiv b \pmod{cn}$, *then* $a \equiv b \pmod{n}$.

7.1. **Modular Linear Equations.** Let $n > 1$ be a natural number. This subsection deals with linear equations (of the form $ax = b$) modulo n.

Proposition 7.5. *If $(a, n) = 1$, then the equation*

$$ax \equiv b \pmod{n} \tag{1}$$

has a unique solution (modulo n).

Proof. Write $\alpha a + \beta n = 1$; then $\alpha a \equiv 1 \pmod{n}$. Then from $ax \equiv b$ it follows that $x \equiv \alpha a x \equiv \alpha b$, which proves the uniqueness. On the other hand $x \equiv \alpha b$ is indeed a solution to the original equation. □

Proposition 7.6. *Let a, b be integers, and $d = (a, n)$. If $d|b$, then the equation (1) is equivalent to $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. Otherwise, it has no solutions.*

Proof. Write $a = da'$ and $n = dn'$. Then the equation becomes $n'd|(a'dx - b)$, which is obviously possible only if $d|b$. If this is the case, write $b = db'$, to get the equation $dn'|(da'x - db')$ which is equivalent to $n'|(a'x - b')$, namely $a'x \equiv b' \pmod{n'}$. □

Notice that the equation given in this proposition is of the type discussed in Proposition 7.5. We conclude that every equation (1) is equivalent to such an equation in which $(a, n) = 1$, and thus have a unique solution (modulo n). Moreover, these equations can always be transferred to an equation with $a = 1$.

Proposition 7.7. *Suppose $(n, m) = 1$. If $n|a$ and $m|a$ then $nm|a$.*

Proof. Since $n|a$ we can write $a = na'$ for some $a' \in \mathbb{Z}$. But then from $m|na'$ it follows (by Proposition 4.17) that $m|a'$, so that $nm|na' = a$. □

We move to treat pairs of such equations.

Theorem 7.8 (Chinese Remaindering Theorem)**.** *Suppose $(n, m) = 1$. Then for every a, b, the equations*

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

have a unique solution modulo nm.

Proof. Let α, β be numbers such that $\alpha n + \beta m = 1$, and let $t = \alpha nb + \beta ma$. Then $t = \alpha nb + (1 - \alpha n)a \equiv a \pmod{n}$, and $t = (1 - \beta m)b + \beta ma \equiv b \pmod{m}$ — so $x = t$ is a solution to this system of equations.

Now assume t' is another solution. Then $t' \equiv a \equiv t \pmod{n}$ and $t' \equiv b \equiv t \pmod{m}$, showing that n, m both divide $t' - t$. But then $nm | t' - t$ by Proposition 7.7, and $t' \equiv t \pmod{nm}$. □

Corollary 7.9. *If $n_1, \ldots, n_t$ are pairwise co-prime, then for every $a_1, \ldots, a_t$ there is a solution to the system of equations*

$$x \equiv a_i \pmod{n_i},$$

which is unique modulo $n = n_1 \ldots n_t$.

Proof. Induction on t. For $t = 1$ there is nothing to prove, and for $t = 2$ the result is Theorem 7.8. Assume the result holds for $t-1$, then there is a solution x' to $x' \equiv a_1 \pmod{n_1}$, ..., $x' \equiv a_{t-1} \pmod{n_{t-1}}$, unique modulo $n' = n_1 \ldots n_{t-1}$. Note that $(n', n_t) = 1$ by Corollary 4.25. Now use Theorem 7.8 for the pair $x \equiv x' \pmod{n'}$ and $x \equiv a_t \pmod{n_t}$ to obtain a unique solution modulo $n_t n' = n$. □

The proof of Theorem 7.8 provides an algorithm to solve the system of equations. Notice that if n, m are fixed (and a, b vary), pre-process which only depends on n, m will enable to solve any system of equations in only two modular multiplications and one addition.

8. Fermat's little theorem

Definition 8.1. *For $n \in \mathbb{N}$, n factorial is defined as $n! = 1 \cdot 2 \cdot \cdots \cdot n$. We also set $0! = 1$.*

Notice that $n! = n \cdot (n-1)!$ for every $n \geq 1$. The first few values of the factorial function are $0! = 1$, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$, $6! = 720$, $7! = 5040$, $8! = 40320$, $9! = 362880$.

Definition 8.2. *If $0 \leq m \leq n$, we set*

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}.$$

This is the number of subsets of size m of a set of size n.

Remark 8.3. *1. We have that $\binom{n}{0} = \binom{n}{n} = \frac{n!}{n!0!} = 1$.*
2. For every $0 \leq m \leq n$, $\binom{n}{n-m} = \binom{n}{m}$.

Example 8.4. *For every n, $\binom{n}{1} = n$. Also, $\binom{6}{3} = \frac{6!}{3!3!} = \frac{720}{6^2} = 20$.*

Exercise 8.5. *Prove that*

$$\binom{n}{m} + \binom{n}{m+1} = \binom{n+1}{m+1}.$$

Corollary 8.6. *$\binom{n}{m}$ is always an integer (by induction on n using the exercise, or according to the combinatorial interpretation).*

We can now easily prove Newton's binomial expansion theorem.

Theorem 8.7 (Newton's binomial formula)**.** *For every a, b and $n \geq 0$, we have that*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Proof. For $n = 0$ the claim is $(a+b)^0 = \binom{0}{0} a^0 b^0$ which is obviously true. Now assume the equality holds for $n \geq 0$, and check it for $n+1$:

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n-k+1} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \binom{n}{n} a^{n+1} b^0 + \binom{n}{0} a^0 b^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a^k b^{n-k+1} + \sum_{k=1}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \binom{n}{n} a^{n+1} b^0 + \binom{n}{0} a^0 b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n-k+1} \\
&= \binom{n}{n} a^{n+1} b^0 + \binom{n}{0} a^0 b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n-k+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n-k+1}.
\end{aligned}$$

□

Proposition 8.8. *If p is a prime and $0 < k < p$, then $\binom{p}{k} \equiv 0 \pmod{p}$.*

Proof. p divides the denominator $p!$ of $\binom{p}{k}$, and is prime to the denominator $k!(p-k)!$; thus, it divides the quotient. □

Corollary 8.9. *If p is prime, then $(a+b)^p \equiv a^p + b^p \pmod{p}$.*

Proof.

$$\begin{aligned}(a+b)^p &= \sum_{k=0} p\binom{p}{k}a^k b^{p-k} \\ &= \binom{p}{p}a^p + \binom{p}{0}b^p + \sum_{k=1} p-1\binom{p}{k}a^k b^{p-k} \\ &\equiv a^p + b^p \pmod p.\end{aligned}$$

□

One corollary is the following theorem of Fermat.

Theorem 8.10 (Fermat's Little Theorem)**.** *For every prime p and every a, $a^p \equiv a \pmod p$.*

Proof. For $a = 0$ the claim is obviously true. Assume the equality holds for a, then

$$(a+1)^p \equiv a^p + 1^p \equiv a + 1 \pmod p,$$

proving the claim by induction. □

Modular exponentiation is an important operation. Though at first sight one may think that the computation of $a^k \pmod n$ requires k modular multiplications, in fact it needs much less than that.

Algorithm 8.11 (Modular exponentiation)**.** *Computing $a^k \pmod n$ in no more than $2\log_2(k)$ modular multiplications.*

Write $k = k_0 + 2k_1 + 4k_2 + \ldots 2^t k_t$ for $t = [\log_2(k)]$ (so that $k_t = 1$). Set $i = t$ and $g = 1$.

1. *If $i = 0$ output g.*
2. *Let $g = g^2$.*
3. *If $k_i = 1$, let $g = a \cdot g$.*
4. *Reduce i by 1, and goto Step 1.*

Exercise 8.12. *Compute $6^{100} \pmod{17}$.*

9. Quadratic Residues modulo primes

Let $p > 2$ be a prime. A number a is called a *quadratic residue* modulo p, if the equation

$$x^2 \equiv a \pmod p \tag{2}$$

has a solution. Otherwise it is called a *quadratic non-residue*. Accordingly, we define the *quadratic residue symbol*:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ is a quadratic residue modulo } p, \\ -1 & \text{otherwise.}\end{cases}$$

Remark 9.1. *Assume that Equation (2) has a solution for $a \not\equiv 0$, then it has precisely two solutions.*

Proof. If $x^2 \equiv a$ then also $(-x)^2 \equiv a$, so there are at least two solutions. On the other hand if $x^2 \equiv y^2$ then $(x-y)(x+y) \equiv 0$ and $y \equiv \pm x$. □

Corollary 9.2. *The only solutions to the equation $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1$.*

Example 9.3. *This statement is not true modulo a composite number n. For example, $1^2 \equiv 4^2 \equiv 11^2 \equiv 14^2 \equiv 1 \pmod{15}$.*

From Remark 9.1 it follows that the $p-1$ non-zero residues have $\frac{p-1}{2}$ different squares, so we obtain

Corollary 9.4. *Out of the $p-1$ non-zero residues mod p, half are quadratic residues, and half are not.*

We need a criterion to distinguish residues from non-residues. Since $a^{p-1} \equiv 1 \pmod{p}$ for every $a \not\equiv 0$, we must have that $a^{\frac{p-1}{2}} \equiv \pm 1$ (see Remark 9.2). Fortunately, the sign determines the quadratic nature of a:

Proposition 9.5. *If $a \neq 0$ is a quadratic residue, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Proof. Write $a \equiv x^2$, then $x \not\equiv 0$ and $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$. □

The number b is called an inverse modulo n of a, if $ab \equiv 1 \pmod{n}$. We start with an easy remark:

Remark 9.6. *If an inverse exists, then it is unique (for if $ab \equiv ab' \equiv 1$, then $b \equiv b(ab') = (ba)b' \equiv b'$).*

Theorem 9.7. *If a is prime to n, then it has an inverse modulo n.*

Proof. Write $\alpha a + \beta n = 1$, then $\alpha a \equiv 1 \pmod{n}$. □

If p is a prime then every number which is not divisible by p is prime to p, so we have

Corollary 9.8. *Every $a \not\equiv 0 \pmod{p}$ has an inverse.*

Theorem 9.9 (Wilson's Theorem)**.** *For every prime p,*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Match the numbers $1, \ldots, p-1$ into pairs $\{x, x^{-1}\}$. The only cases with $x \equiv x^{-1}$ are when $x^2 \equiv 1$, namely $x = 1, -1$. Thus the product of the numbers $1, \ldots, p-1$ is the product over all the pairs (which is 1), multiplied by 1 and by -1. □

Using a similar idea we can prove the following result.

Proposition 9.10. *If $a \neq 0$ is a quadratic non-residue, then $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

Proof. Divide the numbers $1, \ldots, p-1$ into pairs $\{x, ax^{-1}\}$. Since a is not a quadratic residue, it never happens that $x \equiv ax^{-1}$, so these are all proper pairs. Now, the product over $1, \ldots, p-1$ is on one hand the product over the $(p-1)/2$ pairs which equals $a^{(p-1)/2}$, and on the other hand is $(p-1)! \equiv -1$ by Wilson's theorem. □

Corollary 9.11. *Together with Proposition 9.5, we proved that*

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}.$$

Corollary 9.12. *The quadratic residue symbol is multiplicative:*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Since $(-1)(-1) = 1$, we in particular obtain

Corollary 9.13. *If a, b are quadratic non-residues, then ab is a quadratic residue.*

Corollary 9.11 makes it easy to reveal the quadratic nature of $-1 \mod p$:

Proposition 9.14. *-1 is a quadratic residue modulo p iff $p \equiv 1 \pmod{4}$.*

Proof. Obviously $(p-1)/2$ is even iff $p \equiv 1 \pmod{4}$. Thus $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \equiv 1$ iff $p \equiv 1 \pmod{4}$. □

Finding the quadratic root, even if such a root exists, is not always easy. For primes which are equivalent to $-1 \pmod{4}$ we can, though, supply a relatively efficient algorithm.

Remark 9.15. *If $p \equiv -1 \pmod{4}$ is a prime, then for every $a \not\equiv 0$, either a or $-a$ (but not both) are quadratic residues.*

Proof. Follows from Corollary 9.12 and the fact that -1 is a quadratic non-residue. □

Proposition 9.16. *Let $p \equiv -1 \pmod{4}$ be a prime. Then $a^{\frac{p+1}{4}}$ is a root of a or $-a$.*

Proof. Let $b = a^{\frac{p+1}{4}}$. Then $b^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}}a = \pm a$. □

Example 9.17. *Let $p = 23$ and $a = 6$. The square root of either 6 or -6 (whichever has a root) is $6^{\frac{23+1}{4}} = 6^6 = 36^3 \equiv (-10)^3 \equiv -8 \cdot 125 \cdot -8 \cdot 10 = -80 \equiv 12 \pmod{p}$. Indeed, $12^2 = 144 \equiv 6$, so 6 is a quadratic residue after all.*

There is no similarly-efficient algorithm for finding square roots modulo primes which are $\equiv 1 \pmod 4$.

There is an interesting formula for the square root of -1 (when $p \equiv 1 \pmod 4$), which is however very inefficient.

Proposition 9.18. *Assume that $p \equiv 1 \pmod 4$, then for $s = \left(\frac{p-1}{2}\right)!$, we have that $s^2 \equiv -1$.*

Proof. By Wilson's theorem $1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \equiv -1 \pmod p$. Ordering this product into pairs $a, -a$ for $a = 1, \ldots, \frac{p-1}{2}$, the product becomes

$$-1 \equiv (p-1)! \equiv (-1)^{\frac{p-1}{2}} (\frac{p-1}{2})!^2 = s^2$$

since $(p-1)/2$ is even by assumption. □

Notice that for $p \equiv -1 \pmod 4$, the same number s satisfies $s^2 \equiv 1$ so that $s \equiv \pm 1$. The exact value depends on the number of quadratic residues among $1, \ldots, (p-1)/2$.

Example 9.19. *Let $p = 13$, and compute that $\left(\frac{p-1}{2}\right)! = 6! = (2\,6)(3\,4)5 \equiv 5$. Indeed, $5^2 = 25 \equiv -1 \pmod{13}$.*

Likewise for $p = 17$ we have that $8! = (2\,8)(3\,6)(5\,7)4 \equiv -4$, and indeed -4 is an (easy to guess) root of -1 modulo 17.

On the other hand, modulo $p = 19$ we have that $9! = (2\,9)(3\,6)(4\,5)(7\,8) \equiv (-1)(-1)(1)(-1) = -1$.

10. Euler's function ϕ

Fix an integer n. In Theorem 9.7 we have seen that numbers which are prime to n have an inverse. We note that the condition is necessary:

Remark 10.1. *If a is not prime to n, then it does not have an inverse.*

Proof. If a has an inverse b, then $n | (ab - 1)$. Let $d = (a, n)$, then $d | n | (ab - 1)$ and $d | a | ab$, so that $d | 1$ and $d = 1$. □

This observation motivates us to define

$$U_n = \{1 \leq a \leq n : (a, n) = 1\}.$$

The set U_n is closed under multiplication modulo n (see Proposition 4.25), and every element of U_n has an inverse 9.7. (such a set is called a *group*).

We use U_n to define a function, called Euler's ϕ, as follows:

$$\phi(n) = |U_n|. \tag{3}$$

Example 10.2. *If p is prime, then $\phi(p) = p-1$ (since all the residues but 0 are prime to p). More values of ϕ are given in Figure 3.*

n	1	2	3	4	6	8	9	10	12	14	16	18	20
$\phi(n)$	1	1	2	2	2	4	6	4	4	6	8	6	8

FIGURE 3. Values of ϕ

Proposition 10.3. *If $n = p^t$ is a prime-power, then $\phi(n) = p^{t-1}(p-1)$.*

Proof. A number $0 \leq a < n$ is not prime to p^t iff it is divisible by p, and there are p^{t-1} such numbers. Thus $\phi(p^t) = p^t - p^{t-1} = (p-1)p^{t-1}$. □

Exercise 10.4. *Prove that $\phi(n)$ is even for every $n \neq 1, 2$.*

Proof. Let $n > 1$. If a is prime to n, then so is $n - a$; so the prime-to-n residues come in pairs, unless for some a we have that $a = n - a$, namely that $a = n/2$ is prime to n. But then $n/2 = (n/2, n) = 1$ (since $n/2$ divides n), and $n = 2$. □

Armed with the new function, we can generalize Fermat's theorem 8.10.

Theorem 10.5. *Let a be any number prime to n. Then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. Let $\{b_1, \ldots, b_{\phi(n)}\}$ denote the residues prime to n, and consider the numbers $\{ab_1, \ldots, ab_{\phi(n)}\}$. To see that they all different modulo n, recall (Proposition 9.7) that a has an inverse a' modulo n, so if $ab_i = ab_j$, then necessarily $b_i \equiv a'ab_i \equiv a' \equiv a'ab_j \equiv b_j$.

The number $N = b_1 \cdots b_{\phi(n)}$ is prime to n, and is equivalent to $(ab_1)\ldots(ab_{\phi(n)}) = a^{\phi(n)}N$, showing that $a^{\phi(n)} = 1$ as claimed. □

As a special case we obtain Fermat's theorem, since for a prime p we have that $\phi(p) = p - 1$.

Proposition 10.6. *If $n|m$, then $\phi(nm) = n\phi(m)$.*

Proof. If a number a is prime to nm, then it is certainly prime to m. On the other hand if $(a, m) = 1$ then $(a, n)|(a, m) = 1$, and by Proposition 4.25 a is prime to nm.

Let $U_m = \{b_1, \ldots, b_t\}$ where $t = \phi(m)$. We claim that $U_{nm} = \{km + b_i : 0 \leq k < n,\ i = 1, \ldots, t\}$, and then $|U_{nm}| = n|U_m|$. □

A function $f:\mathbb{N}\to\mathbb{Z}$ is called *multiplicative* if $f(nm)=f(n)f(m)$ whenever $(n,m)=1$.

Theorem 10.7. *Euler's ϕ is multiplicative, namely if n,m are co-prime then*

$$\phi(nm)=\phi(n)\phi(m).$$

Proof. Let n,m be co-prime numbers. Consider the correspondence (established by the Chinese Remaindering Theorem) from a residue $x \pmod{nm}$ to the pair of its residues modulo n,m.

We are thus done by checking that if x is prime to nm then it is prime to n,m (which is obvious), and if it is prime to m,n then it is prime to mn (which is Proposition 4.25). □

This information suffices for a useful formula for $\phi(n)$.

Proposition 10.8. *Let $n=p_1^{\alpha_1}\cdots p_t^{\alpha_t}$.*

Then

$$\phi(n)=(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_t})n \tag{4}$$

Proof. We have that

$$\phi(n)=\prod_i(p_i^{\alpha_i-1}(p_i-1))=\prod_i(p^i(1-\frac{1}{p_i}))=n\prod_i(1-\frac{1}{p_i}).$$

□

Exercise 10.9. *Find all the numbers n such that $\phi(n)=2,4,6$.*

Exercise 10.10. *Solve the equation*

$$\phi(2n)=\frac{\phi(3n)+\phi(n)}{2}.$$

Solution. Let $q_1=\phi(2n)/\phi(n)$, and $q_2=\phi(3n)/\phi(n)$; then $q_1=2,1$ according to whether or not 2 divides n. Likewise $q_2=3,2$ according to whether or not 3 divides n. The equation then becomes $2q_1=q_2+1$, so either $q_1=q_2=1$ or $q_1=2$ and $q_2=3$.

The solutions are, then, all the numbers which are either divisible by 6 or prime to 6. □

10.1. **Order modulo n.** Let $a\in U_n$. The *order* of a modulo n is defined as the least $e>0$ such that $a^e\equiv 1 \pmod{n}$. Such a number always exists (and is $\leq\phi(n)$) by Theorem 10.5.

Proposition 10.11. *The order of $a\in U_n$ always divides $\phi(n)$.*

Proof. Let e denote the order of a, and divide $\phi(n)$ by e: $\phi(n) = qe + r$ where $0 \leq r < e$. Now $a^r = a^{\phi(n)-qe} = a^{\phi(n)}(a^e)^{-q} \equiv 1$. By the minimality of e, we must have that $r = 0$ and $e|\phi(n)$. □

Example 10.12. *Modulo $p = 13$, the orders are as follows:*

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ord}_{13}(a)$	1	12	3	6	4	12	12	4	3	6	12	2

It turns out (though we shall not prove it here) that if n is a prime, there are $a \in U_n$ with order equal to $\phi(n) = n-1$. This property (that U_n has elements of order n) is special for the numbers $1, 2, 4, p^k, 2p^k$ where p is an odd prime and k is arbitrary. For other numbers, the maximal order is smaller, and we will now define a function related to this maximal order.

We use $\mathrm{lcm}(a, b)$ to denote the least common multiple of a, b.

Definition 10.13. *Define a function $\lambda : \mathbb{N} \to \mathbb{N}$ be $\lambda(1) = \lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^k) = 2^{k-2}$ for $k \geq 3$, and $\lambda(p^k) = p^{k-1}(p-1)$ for p an odd prime and $k \leq 1$.*

More generally if $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ where p_i are distinct primes, then

$$\lambda(n) = \mathrm{lcm}(\lambda(p_1^{\alpha_1}), \dots, \lambda(p_t^{\alpha_t})).$$

Example 10.14. *Let $n = 9520$. Since $9520 = 2^4 \cdot 5 \cdot 7 \cdot 17$, we have that*

$$\phi(9520) = \phi(16) \cdot \phi(5)\phi(7)\phi(17) = 8 \cdot 4 \cdot 6 \cdot 16 = 3072$$

while

$$\lambda(9520) = \mathrm{lcm}(\lambda(16), \lambda(5), \lambda(7), \lambda(17)) = \mathrm{lcm}(8, 4, 6, 16) = 48.$$

The obvious relation between $\lambda(n)$ and $\phi(n)$ is the following:

Proposition 10.15. *For every n, $\lambda(n)|\phi(n)$.*

Proof. If n is an odd prime power, then $\lambda(n) = \phi(n)$, and if $n = 2^k$ then $\lambda(n)|\phi(n)$ by definition.

In general, write $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, then $\lambda(n)$ is the least common multiple of the numbers $\lambda(p_i^{\alpha_i})$, while $\phi(n)$ is the product of the $\phi(p_i^{\alpha_i})$ which is certainly divisible by any $\lambda(p_i^{\alpha_i})$. □

The difficult part in Theorem 10.18 is the following:

Proposition 10.16. *Let $k \geq 3$, $n = 2^k$, and a an odd number. Then*

$$a^{n/4} \equiv 1 \pmod{n}.$$

Proof. Recall that in Theorem 10.5 we proved that $a^{n/2} \equiv 1 \pmod{n}$.

We claim that for $g \geq 1$, if $s \equiv \pm 1 \pmod{2^g}$, then $s^2 \equiv 1 \pmod{2^{g+1}}$. Indeed, write $s = 2^g u \pm 1$, then $s^2 \equiv 2^{2g}u^2 \pm 2^{g+1}u + 1 \equiv 1 \pmod{2^{g+1}}$.

Now, since a is odd, $a-1$ and $a+1$ are even. Moreover, one of these numbers must be divisible by 4. Thus $a \equiv \pm 1 \pmod{4}$, $a^2 \equiv 1 \pmod{2^3}$, $a^{2^2} \equiv 1 \pmod{2^4}$, and by induction on i, $a^{2^i} \equiv 1 \pmod{2^{i+2}}$. Putting $i = k-2$ we get $a^{n/4} \equiv 1 \pmod{n}$, as asserted. □

Corollary 10.17. *If n is a prime power and $a \in U_n$, then $a^{\lambda(n)} \equiv 1 \pmod{n}$.*

Proof. If n is an odd prime power this follows from Theorem 10.5 (as $\phi(n) = \lambda(n)$. If n is a power of 2, use the last proposition. □

We can now prove the most important property of the function λ:

Theorem 10.18. *For every a prime to n, we have that*

$$a^{\lambda(n)} \equiv 1 \pmod{n}.$$

Proof. Let $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$. To show that $a^{\lambda(n)} \equiv 1 \pmod{n}$, it is enough (by Theorem 7.8) to show that $a^{\lambda(n)} \equiv 1 \pmod{p_i^{\alpha_i}}$ for every $i = 1, \dots, t$.

But for every i, $\lambda(p_i^{\alpha_i}) | \lambda(n)$, so that $a^{\lambda(n)} \equiv (a^{\lambda(p_i^{\alpha_i})})^{\lambda(n)/\lambda(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$. □

Exercise 10.19. *Find all the numbers n for which $\lambda(n) \leq 4$.*

We end this section by proving an interesting property of the function ϕ.

Theorem 10.20. *For every n, we have that $\sum_{d|n} \phi(d) = n$.*

Proof. Divide the n residues $0, 1, 2, \dots, n$ to classes, according to their greatest common divisor with n: let $A_d = \{0 \leq a \leq n : (a, n) = d\}$. This is obviously a disjoint partition of $\{0, 1, \dots, n\}$, so that $\sum_d |A_d|$ (where the sum is over $d|n$ since the greatest common divisor always divides d.

We claim that $|A_d| = \phi(n/d)$. Indeed, $(a, n) = d$ iff $d|a$ and $(a/d, n/d) = 1$; so there is a one-to-one correspondence between residues modulo n/d which are prime to n/d, and residues modulo n with $(a, n) = d$. This proves that $n = \sum_d \phi(n/d)$, so setting n/d in place of d we get the desired result. □

Remark 10.21. *Concerning the average behaviour of $\phi(n)$, it was proved by Mertens (1874) that $\frac{1}{n}\sum_{k=1} n\phi(k) = \frac{3}{\pi^2}n + O(\log(n))$.*

Landau (1902) showed that $\phi(n)$ is bounded from below by a constant times $\frac{n}{\log\log n}$, more precisely that the infimum limit of $\phi(n)/(n/\log\log(n))$

is $e^{-\gamma}$ *where* γ *is Euler's constant* $= \lim_{n\to\infty} 1 + 1/2 + \cdots + 1/n - \log(n)$. *He also proved (1909) that* $\limsup \log(\tau(n))/(\log(n)/\log\log(n)) = \log(2)$.

11. Pseudo primes

It turns out that factorization methods take relatively long (non-polynomial) time, and the first step in any attempt to factorize a number should be to make sure it is not a prime (which is much quicker). With very low probability of error, this can be done in polynomial time (in fact, there are also polynomial time deterministic algorithms to test primality, but we will not present them here).

If n is large, the reasonable first step in testing if its a prime is to try division by small numbers. This is done very quickly even if n is huge.

We know that if n is a prime, then for every a we should have that $a^{n-1} \equiv 1 \pmod{n}$. This is an efficient test, since computing $a^{n-1} \pmod{n}$ only takes about $\log(n)$ modular multiplications.

Of course, if $a^{n-1} \not\equiv 1 \pmod{n}$, we immediately know that n is not a prime. The reverse direction frequently holds, but not always.

Definition 11.1. *If* n *is composite and* $a^{n-1} \equiv 1 \pmod{n}$, *then* n *is called a pseudo-prime for the basis* a.

Example 11.2. *Let* $n = 341$ *and* $a = 2$. *Since* $3n + 1 = 1024 = 2^{10}$, *we have that* $2^{10} \equiv 1 \pmod{n}$ *so surely* $2^{340} \equiv 1 \pmod{n}$.

However $341 = 11 \cdot 31$, *so* 341 *is a pseudo-prime for the basis* 2.

We can put the definition in the form of a test, as follows.

Test 11.3. *Given* n *and* $1 < a < n$, *we want to check if* n *is a prime.*

1. *Compute* $d = (n, a)$. *If* $d > 1$ *then* n *is composite.*
2. *Compute* $a^{n-1} \pmod{n}$. *If the result is not* $\equiv 1 \pmod{n}$, *declare* n *to be composite. Otherwise,* n *is either a prime or a pseudo-prime to basis* a.

Regarding primality testing we may assume n is odd. Also, modulo a prime, the only roots of 1 are 1 and -1. This results in the following improved test:

Test 11.4. *Given* n *and* $1 < a < n$, *we want to check if* n *is a prime.*

1. *Compute* $d = (n, a)$. *If* $d > 1$ *then* n *is composite.*
2. *Write* $n - 1 = 2^\alpha m$, *where* m *is odd.*
3. *Compute the number* $a^m \pmod{n}$. *If the result is* 1, *declare* n *to be a strong pseudo-prime (for basis* a*).*
4. *Compute (by squaring) the numbers* $a^{2m}, a^{4m}, \ldots, a^{2^\alpha m} \pmod{n}$. *If* $a^{2^\alpha m} = a^{n-1} \not\equiv 1 \pmod{n}$, *declare* n *to be composite.*

5. *Let i be the maximal such that $a^{2^i m} \not\equiv 1 \pmod{n}$. If $a^{2^i m} \not\equiv -1$, declare n to be composite. Otherwise n is a prime, or a strong pseudo-prime.*

Proposition 11.5. *A strong pseudo-prime is, in particular, a pseudo-prime (for the same basis).*

Proof. If $a^{n-1} \not\equiv 1 \pmod{n}$ then n is declared composite by step 4 of Test 11.4. □

It is known that for any base a there are infinitely many strong pseudo-primes (though we shall not prove this difficult result here).

It is more rare for a number to be a pseudo-primes for every base:

Definition 11.6. *A composite n is called a Charmichael number if $a^{n-1} \equiv 1 \pmod{n}$ for every a which is prime to n.*

Which numbers are bound to satisfy this property? Recall from Theorem 10.18 that $a^{\lambda(n)} \equiv 1 \pmod{n}$ for every a prime to n.

Corollary 11.7. *If n is not a prime and $\lambda(n)|(n-1)$, then n is a Charmichael number.*

Example 11.8. *$n = 561 = 3 \cdot 11 \cdot 17$ is a Charmichael number, since $\lambda(561) = \mathrm{lcm}(2, 10, 16) = 80$ divides $n - 1 = 7 \cdot 80$.*

We can deduce various properties of Charmichael numbers assuming that U_n has elements of order $\lambda(n)$, which we did not prove yet. From this assumption it follows that a composite n is a Charmichael number iff $\lambda(n)|(n-1)$.

Proposition 11.9. *A Charmichael number:*

a. must be odd.

b. cannot have repeated prime factors.

c. must have at least three prime factors.

Proof. a. Since $n > 2$, $\lambda(n)$ is even and cannot divide $n - 1$ unless n is odd.

b. If $p^2|n$ then $p|\lambda(n)$, but p does not divide $n - 1$.

c. Suppose that $n = pq$, then $\lambda(n) = \mathrm{lcm}(p-1, q-1)$ should divide $n - 1 = (pq - 1)$. But if $p - 1|(pq - 1) = (p-1)q + (q-1)$ then $p - 1|q - 1$, and likewise $q - 1|p - 1$, which shows that $p = q$. □

Example 11.10. *If $6m+1, 12m+1$ and $18m+1$ are all primes, $n = (6m+1)(12m+1)(18m+1)$ is a Charmichael number.*

This follows since $\lambda(n) = \mathrm{lcm}(\lambda(6m+1), \lambda(12m+1), \lambda(18m+1)) = \mathrm{lcm}(6m, 12m, 18m) = 36m$, which divides $n - 1 = (6m+1)(12m+1)(18m+1) = 36m(36m^2 + 11m + 1)$.

Remark 11.11. *If a, b, c are numbers such that $n = (am+1)(bm+1)(cm+1)$ is a Charmichael number whenever $am+1, bm+1, cm+1$ are primes, then up to reordering $b = 2a$ and $c = 3a$, and $6|a$.*

Proof. Assume that $am+1, bm+1, cm+1$ are all primes. Then am needs to divide $n-1 = abcm^3 + (ab+bc+ca)m^2 + (a+b+c)m$, which is equivalent to a dividing $bcm + (b+c)$, and (since this is supposed to be the case for arbitrary values of m; we omit some details here) $a|bc$ and $a|b+c$. Likewise $b|ac$, $b|a+c$ and $c|ab$, $c|a+b$.

Since n cannot have repeated factors, we may assume that $a < b < c$. But then $c|a+b < 2c$ forces $c = a+b$. Hence, $b|a+c = 2a+b$ so that $b|2a$ and $b = 2a$; and so $c = 3a$. Now $c = 3a|ab = 2a^2$ so that $3|a$, and similarly $b = 2a|ac = 3a^2$ so that $2|a$. □

Exercise 11.12. *Show that if $60m+1, 240m+1, 300m+1, 600m+1$ are all primes, then their product is a Charmichael number. An example (the smallest in this family) is $n = 6661 \cdot 26641 \cdot 33301 \cdot 66601$.*

It is known (though quite difficult to show) that there are infinitely many Charmichael numbers. On the other hand it is not known if there are infinitely many numbers of the form of Example 11.10. We also remark that a number cannot be strong pseudo-prime for every basis.

12. Factorization methods

12.1. **Divisibility signs.** We naturally identify a number n with the sequence of decimal digits $a_t a_{t-1} \dots a_0$ representing it, if $n = a_0 + 10a_1 + 10^2 a_2 + \dots 10^t a_t$. Some divisibility conditions take the form of a simple test on the digits.

Divisibility by 2, 5: n is divisible by 2 or 5 iff the last digit a_0 is.

Divisibility by 3, 9: n is equivalent to $a_0 + \dots + a_t$ modulo 9, since $10 \equiv 1 \pmod 9$, and in particular n is divisible by 3 or 9 iff its sum of digits is.

Divisibility by 4: $4|n$ iff $4|(a_0 + 10a_1)$ (since $4|100$).

Divisibility by 11: modulo 11, n is equivalent to $a_0 - a_1 + a_2 - \dots$, so n is divisible by 11 iff the alternating sum of the its digits is.

12.2. **Eratosthenes sieve.** The sieve, invented by Eratosthenes, enables one to list all the primes up to n with roughly $n \cdot \log\log(n)$ operations.

Algorithm 12.1. *We wish to list all the primes up to n.*

In our list, numbers can be either unmarked, or marked as primes, or erased.

1. *List all the numbers from* 2 *to* n.
2. *Let* p *be the smallest unmarked number in the list.*
3. *Mark* p *as a prime.*
4. *Erase from the list all the numbers* $pm \leq n$ *for* $m = p, p+1, p+2, \ldots$.
5. *Goto step 2.*

Notice that step 4 is vacuous for the primes $p > \sqrt{n}$ (and once p reaches that bound, we only mark the remaining numbers as primes).

See Example 3.10 for the list of primes up to 100.

12.3. **Trial division.** The naive way to check if a given number n is a prime: check divisibility by all numbers $m \leq \sqrt{n}$. Number of division operations: $O(\sqrt{n})$.

Proposition 12.2. *If* n *is not a prime, then it has a divisor* $1 < m \leq \sqrt{n}$.

Proof. If $n = ab$ and $a, b > \sqrt{n}$ then we obtain a contradiction from $n = ab > \sqrt{n}^2 = n$. □

12.4. **Equations on squares.** The following basic observation is basic in many modern factorization methods:

Remark 12.3. *If* $x^2 \equiv y^2 \pmod{n}$ *and* $x \not\equiv \pm y$, *then* $(n, x-y)$ *or* $(n, x+y)$ *is a non-trivial divisor of* n.

Proof. For $n|(x^2 - y^2) = (x-y)(x+y)$, but does not divide $x-y$ or $x+y$. Let p be a prime divisor of n, then p divides one of $x-y, x+y$, and accordingly $p|(n, x-y)$ or $p|(n, x+y)$, where these greatest common divisors are not equal to n. □

Use squares: we have that $85^2 \equiv 12^2 \pmod{7081}$ and indeed $7081 = 73 \cdot 97$ (where $85 \pm 12 = 73, 97$).

12.5. **Pollard's ρ method.** We know that if balls are thrown to n bins, where the chances to hit any specific bin are $1/n$, then the 'waiting time' (number of balls needed to be thrown on average) for the first hit at bin #1 is n.

On the other hand, the waiting time for the first collision (two balls hitting the same bin) is only $O(\sqrt{n})$, more precisely $\sqrt{\frac{\pi n}{2}} + 2$ when n is large. This fact is responsible for what is called 'the birthday paradox', that if 24 people meet at random the chances of two of them having the same birthday is more than half.

In slightly different setup, let $f : X \to X$ is a random function on a space X of size n (where by a random function we mean that every

value $f(x)$ is independently chosen at random). Choose a starting point $x_0 \in X$, and apply f again and again, until hitting the same value for the second time. This procedure mimics the previous experiment, and so the waiting time for the path to close is $O(\sqrt{n})$. This observation is in the basis of the following factorization method.

Algorithm 12.4 (Pollard's ρ)**.** *Given n, we wish to find a non-trivial divisor of n.*

1. *Set $r = 1$ and $x_0 = y_0 = r$. Set $k = 0$.*
2. *Set $x_{k+1} = x_k^2 + 2 \pmod n$.*
3. *Set $y_{k+1} = (y_k^2 + 2)^2 + 2 \pmod n$.*
4. *Advance k.*
5. *Compute $d = (n, x_k - y_k)$.*
6. *If $d = 1$, go to step 2. If $d = n$, announce failure (and consider running again with a different r). Otherwise d is a non-trivial factor of n.*

Fix a prime p, and consider the path of $r = 1$ under the pseudo-random $f(x) = x^2 + 2 \pmod p$ (defined by connecting every z to $f(z)$ until a collision is met).

Let T_p denote the length of the tail, and C_p the length of the cycle, and let $s(p)$ denote the smallest number $\geq T_p$ which is divisible by C_p.

It is easy to see that $x_k \equiv y_k \pmod p$ once $k = s(p)$; notice that in this case, $d = (n, x_k - y_k)$ is divisible by p.

From probabilistic analysis we expect that for every prime divisor, $T_p + C_p = O(\sqrt{p})$, and it thus follows that $d > 1$ will occur after $O(\sqrt{p_{\min}})$ steps. (Also notice that the chances of the first collision to occur at the same time modulo two different primes is roughly $O(1/\sqrt{p'})$ where p' is the largest of the two, and for the algorithm to fail the collision must occur at the same step modulo all the primes).

Finally, since the smallest prime factor satisfies $p \leq \sqrt{n}$, the running time of this algorithm is bounded by $O(n^{1/4})$ steps whenever n is composite.

Example 12.5. *We factorize $n = 8051$ using Pollard's ρ method. Setting $r = 1$, we obtain*

$k = 0$	$x_0 = 1$	$y_0 = 1$	
$k = 1$	$x_1 = 3$	$y_1 = 11$	$(n, y_1 - x_1) = 1$
$k = 2$	$x_1 = 11$	$y_1 = 7080$	$(n, y_2 - x_2) = 1$
$k = 3$	$x_1 = 123$	$y_1 = 2533$	$(n, y_3 - x_3) = 1$
$k = 4$	$x_1 = 7080$	$y_1 = 3200$	$(n, y_4 - x_4) = 1$
$k = 5$	$x_1 = 876$	$y_1 = 108$	$(n, y_5 - x_5) = 1$
$k = 6$	$x_1 = 2533$	$y_1 = 1454$	$(n, y_6 - x_6) = 83$

so we get the factor 83; indeed, $n = 8051 = 83 \cdot 97$.

13. Public cryptography

The classical problem of cryptography is to transmit information between two parties A and B, so that a third (unauthorized) party will be unable to retrieve the information.

The basic observation is that any message can be translated to bits (=binary digits, namely number modulo 2). Then, if $K = 0, 1$ is a secret "key" bit shared by the partners and $M = 0, 1$ is the secret bit A wants to deliver to B, she should transmit $K \oplus M = K + M \pmod 2$. He would then compute $(K \oplus M) \oplus K = M$, but for an adversary (who does not know the value of M), the value of $K \oplus M$ gives no information on the secret message M.

Transmitting longer messages can be done in a similar way, where a matching key bit is set for every message bit.

The main problem of public cryptography is how to avoid the need to prior coordination between the parties. More precisely, We describe two solutions to the following problem: how can party A create an asymmetric scheme in which every can encrypt messages (based on public information), while only A himself can decrypt.

13.1. **RSA scheme.** Preparations: choose two (large) primes p, q, and set $n = pq$. Choose a (small) number d which is prime to n. Compute $e \equiv d^{-1} \pmod{\phi(n)}$ (notice that $\phi(n) = (p-1)(q-1)$).

Public information: the numbers n and d.

Private information: the number e.

The messages: numbers modulo n.

To encrypt a message m: compute (and transmit) $r = m^d \pmod n$.

To decrypt r: compute $r^e \pmod n$ (notice that this requires knowledge of e).

Remark 13.1. *The result of decryption is indeed the original message. For* $r^e = (m^d)^e = m^{de} = m^{1+\alpha\phi(n)} = m \cdot (m^{\phi(n)})^\alpha \equiv m \pmod n$ *for an appropriate* α.

Notice that the method properly decipher only messages m which are prime n. The probability of hitting m which is not prime to n at random is very small (only $\frac{n-\phi(n)}{n} = \frac{1}{p} + \frac{1}{q} - \frac{1}{n}$), and in any case if this happens, the number n is factored and the scheme is broken.

Proposition 13.2. *The following problems are equally hard for a number* $n = pq$*: factoring* n*, and computing* $\phi(n)$.

Proof. ¿From the prime factors we easily compute $\phi(n) = n-(p+q-1)$. On the other hand, given $\phi(n)$, the prime factors p, q solve the equation

$$x^2 - (n - \phi(n) + 1)x + n = 0$$

and can thus be found by a single square-root operation. □

However, it is not known if being able to 'break' the RSA scheme (i.e. decipher some non-negligible percentage of messages encrypted in this way) is as hard as factoring n.

13.2. **Rabin's shceme.** In this similar method, the encryption process is a bit faster than in RSA, and it is also theoretically more secure, as breaking it is known to be equivalent to factorization. On the other hand the decryption is more complicated.

Preparations: choose two (large) primes $p, q \equiv 3 \pmod 4$, and set $n = pq$. Find α, β such that $\alpha p + \beta q = 1$.

Public information: the number n.

Private information: the factors p, q.

The messages: numbers modulo n, with redundancy (e.g. numbers which end with binary ...0000000000000001).

To encrypt a message m: compute (and transmit) $r = m^2 \pmod n$.

To decrypt r: compute $a = \sqrt{r} \pmod p$ and $b = \sqrt{r} \pmod q$ (using Proposition 9.16). To find m modulo n, check which of the four numbers $\pm\alpha pb \pm \beta qa \pmod n$ has the redundancy property (the three others are expected to look 'random').

14. Number theoretic functions

Let $f, g : \mathbb{N} \to \mathbb{Z}$ be functions. We define a new function $f * g$, as follows:

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

Example 14.1.

$$\begin{aligned}
(f*g)(1) &= f(1)g(1) \\
(f*g)(p) &= f(1)g(p) + f(p)g(1) \qquad \textit{for prime } p \\
(f*g)(9) &= f(1)g(9) + f(3)g(3) + f(9)g(1) \\
(f*g)(12) &= f(1)g(12) + f(2)g(6) + f(3)g(4) + \cdots + f(12)g(1)
\end{aligned}$$

Proposition 14.2. *We have that $f * g = g * f$ (commutativity) and $f * (g * h) = (f * g) * h$ (associativity).*

Let us define some special functions:

$$\delta_1(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

$$\mathcal{C}(n) = 1.$$

$$\mathcal{I}(n) = n.$$

Example 14.3.

$$\begin{aligned}(\mathcal{C} * \mathcal{C})(6) &= \mathcal{C}(1)\mathcal{C}(6) + \mathcal{C}(2)\mathcal{C}(3) + \mathcal{C}(3)\mathcal{C}(2) + \mathcal{C}(6)\mathcal{C}(1)\\ &= 1 + 1 + 1 + 1 = 4,\\ (\mathcal{I} * \delta_1)(6) &= \mathcal{I}(1)\delta_1(6) + \mathcal{I}(2)\delta_1(3) + \mathcal{I}(3)\delta_1(2) + \mathcal{I}(6)\delta_1(1)\\ &= 0 + 0 + 0 + 6 = 6.\end{aligned}$$

The function δ_1 serves as a unit for the operation $*$:

Proposition 14.4. *For every function f, we have that $\delta_1 * f = f$.*

Proof. By definition $(\delta_1 * f)(n)$ is the sum of values $\delta_1(d)f(n/d)$ over the divisors $d|n$. But $\delta_1(d) = 0$ unless $d = 1$, so the only non-zero term in the sum is $\delta_1(1)f(n) = f(n)$ and $(\delta_1 * f)(n) = f(n)$. □

With a unit at hand, we can define the inverse:

Definition 14.5. *g is called an inverse of f, if $f * g = \delta_1$.*

Exercise 14.6. *Prove that if an inverse to f exists, then it is unique.*

The inverse of f is denoted by f^{-1}.

Theorem 14.7. *A function $f : \mathbb{N} \to \mathbb{Z}$ has an inverse iff $f(1) = \pm 1$.*

Proof. First, if $f * g = \delta_1$, then $1 = \delta_1(1) = (f * g)(1) = f(1)g(1)$ so that $g(1)$ is the inverse of the number $f(1)$, and $f(1)$ must be 1 or -1.

Now assume $f(1) = \pm 1$; we define the function g by induction. Set $g(1) = f(1)$. Now assume $g(m)$ is defined for every $1 \leq m < n$, and choose $g(n) = -f(1) \sum_{d|n, d<n} f(n/d)g(d)$.

To prove that $f * g = \delta_1$, check that $(f * g)(1) = f(1)^2 = 1$, and for $n > 1$ we by definition have $(f*g)(n) = \sum_{d|n} f(n/d)g(d) = f(1)g(n) + \sum_{d|n, d<n} f(n/d)g(d) = f(1)g(n) - f(1)g(n) = 0$. □

Exercise 14.8. *Given f with $f(1) = 1$, compute the values $f^{-1}(n)$ for $n \leq 10$ in terms of $f(1), \ldots, f(10)$.*

Given a function f, we are often interested in the function

$$F = f * \mathcal{C}, \tag{5}$$

namely $F(n) = \sum_{d|n} f(d)$. Our aim is to reverse this definition, and express f in terms of F. However, using the machinery developed so far, it is enough to find $\mathcal{C}^{-1}$ (since then $F * \mathcal{C}^{-1} = (f * \mathcal{C}) * \mathcal{C}^{-1} = f * \delta_1 = f$).

Definition 14.9. *Möbius function μ is defined as follows:*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ has any repeated factors} \\ (-1)^s & \text{if } n = p_1 \dots p_s \text{ where } p_i \text{ are distinct primes.} \end{cases}$$

The first values of μ or given in Figure 4.

n	1	2	3	4	6	8	9	10	12	14	16	18	20
$\mu(n)$	1	−1	−1	0	1	0	0	1	0	1	0	0	0

FIGURE 4. Values of μ

Theorem 14.10. *The Möbius function is the inverse of $\mathcal{C}$.*

Proof. We need to show that $(\mathcal{C} * \mu) = \delta_1$, namely that $\mu(1) = 1$ (which holds by definition), and that

$$f(n) = \sum_{d|n} \mu(d) = 0$$

for every $n > 1$.

Write $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ where p_i are the distinct prime factors, and let $n_0 = p_1 \dots p_t$. Any divisor $d|n_0$ with no repeated factors, is also a divisor of n_0; it follows that $f(n) = f(n_0)$.

For every $0 \le k \le s$, there are $\binom{s}{k}$ divisors of n_0 which are product of k prime factors, and for them $\mu(d) = (-1)^k$. It follows that

$$f(n_0) = \sum_{k=0}^{s} \binom{k}{s} (-1)^k = (1-1)^s = 0$$

as claimed. □

Exercise 14.11. *Prove that $\sum_{d|n}(-1)^{n/d}\mu(d) = 0$ for every $n > 2$.* **Hint**. *Let $T(n) = (-1)^n$. Prove that $T = (\delta_2 - 2\delta_1) * C$, where δ_2 is defined similarly to δ_1.*

Theorem 14.12. *Let ϕ be Euler's function. Then $\phi * \mathcal{C} = \mathcal{I}$.*

Proof. This is Theorem 10.20. □

We conclude by defining two special functions.

Definition 14.13. *Let $\tau(n)$ denote the number of natural divisors of n (e.g. $\tau(p) = 2$ for a prime p, $\tau(12) = 6$).*

Let $\sigma(n)$ denote the sum of natural divisors of n (e.g. $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$).

Exercise 14.14. *Prove that $\tau = \mathcal{C} * \mathcal{C}$ and that $\sigma = \mathcal{C} * \mathcal{I}$.*

Proposition 14.15. *If $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, then*

$$\tau(n) = (\alpha_1 + 1) \dots (\alpha_t + 1)$$

and

$$\sigma(n) = \frac{p_1^{\alpha_1} - 1}{p_1 - 1} \cdot \dots \cdot \frac{p_t^{\alpha_t} - 1}{p_t - 1}.$$

Proposition 14.16. *We have that $\phi * \tau = \sigma$.*

Proof. Compute that $\phi * \tau = \phi * (\mathcal{C} * \mathcal{C}) = (\phi * \mathcal{C}) * \mathcal{C} = \mathcal{I} * \mathcal{C} = \sigma$. □

A number n with $\sigma(n) = 2n$ is called a *perfect* number. Examples: $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 8 + 14$ are perfect. Another example is $496 = 2^4 \cdot 31$.

Proposition 14.17. *Every even perfect number is of the form $2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are both primes.*

It is not known if there are infinitely many perfect numbers. Likewise, it is not known if there are any odd perfect numbers.

If $\sigma(n) - n = m$ and $\sigma(m) - m = n$, then n, m are called an *amicable* pair. The smallest example is the pair $220, 284$.

14.1. **Multiplicative functions.** A function $f : \mathbb{N} \to \mathbb{Z}$ is called *multiplicative* if for every n, m such that $(n, m) = 1$, we have that $f(nm) = f(n)f(m)$. A function is strongly multiplicative if it satisfies the equation $f(nm) = f(n)f(m)$ for every n, m.

Observe that a multiplicative function is determined by its values on prime powers, and that a strongly multiplicative function is determined by its values on primes.

Example 14.18. *The functions $\delta_1, \mathcal{C}, \mathcal{I}$ are strongly multiplicative.*

Example 14.19. *The Möbius function μ is multiplicative (by its definition), but not strongly multiplicative.*

Theorem 14.20. *If f, g are both multiplicative, then so is $f * g$.*

Proof. Let n, m be co-prime numbers. We need to show that $(f * g)(nm) = (f*g)(n)\cdot(f*g)(m)$. Notice that if $k | nm$, then by Proposition 4.27, $k = (k, nm) = (k, n)(k, m)$, so every divisor of nm is a product of divisors of n, m, which it determines. Moreover, $d = (k, n)$ and $e = (k, m)$ divide n, m respectively, and so they are prime, and the same holds for $n/d, m/e$.

By definition,

$$\begin{aligned}(f*g)(nm) &= \sum_{k|nm} f(k)g(nm/k)\\ &= \sum_{d|n,\,e|m} f(de)g(nm/de)\\ &= \sum_{d|n,\,e|m} f(d)f(e)g(n/d)g(m/e)\\ &= \sum_{d|n} f(d)g(n/d)\cdot\sum_{e|m} f(e)g(m/e)\\ &= (f*g)(n)\cdot(f*g)(m).\end{aligned}$$

□

Remark 14.21. *If f is multiplicative then $f(n)=f(n\cdot 1)=f(n)\cdot f(1)$, showing that $f(1)=1$ unless $f=0$.*

Theorem 14.22. *If $f\neq 0$ is multiplicative, then f^{-1} is multiplicative.*

Proof. Theorem 14.7 gives a formula for the inverse g of f, namely $f(1)=1$ and for every n, $g(n)=-f(1)\sum_{d|n,d<n} f(n/d)g(d)$. We prove that g is multiplicative by induction: first, $1=1\cdot 1$ is the only factorization of 1, and indeed $g(1)=f(1)=1=f(1)^2=g(1)^2$. Assume that for every $u<N$, if $u=u_1u_2$ are co-prime, then $g(u)=g(u_1)g(u_2)$. Now suppose $N=nm$ where n,m are co-prime. Then

$$\begin{aligned}g(nm) &= -\sum_{k|nm,d<nm} f(nm/k)g(k)\\ &= -\sum_{d|n,e|m,de<nm} f(nm/de)g(de)\\ &= -\sum_{d|n,e|m,de<nm} f(n/d)f(m/e)g(d)g(e)\\ &= g(n)g(m)-\sum_{d|n,e|m} f(n/d)f(m/e)g(d)g(e)\\ &= g(n)g(m)-\sum_{d|n} f(n/d)g(d)\cdot\sum_{e|m} f(m/e)g(e)\\ &= g(n)g(m)-0\cdot 0=g(n)g(m).\end{aligned}$$

□

The functions we met so far are all products of $\mathcal{C}$ and $\mathcal{I}$ and their inverses, as the table below shows. In particular they are all multiplicative (recall that it was proved in Theorem 10.7 for ϕ).

	$\mathcal{C}^{-1}$	δ_1	$\mathcal{C}$	$\mathcal{C} * \mathcal{C}$
$\mathcal{I}^{-1}$				
δ_1	μ	δ_1	$\mathcal{C}$	τ
$\mathcal{I}$	ϕ	$\mathcal{I}$	σ	

FIGURE 5. Number theoretic functions

Remark 14.23. *If n, m are not co-prime, then not all the divisors of nm factor as a divisor of n times a divisor of m. It follows that $f * g$ is not necessarily strongly multiplicative, even if f, g are. For example, $\phi = \mathcal{I} * \mu$ is not strongly multiplicative (as $\phi(4) \neq \phi(2)^2$).*

E-mail address: uv2@math.yale.edu