ELEMENTARY NUMBER THEORY

UZI VISHNE

Exercise Set 1. Basic properties

1. Prove (from the axioms of $\mathbb{Z}$) that $0 < 1$.

2. Let $a \in \mathbb{Z}$. Prove (from the axioms) that the element b such that $a + b = 0$ is unique (so the name $-a$ is justified) **Hint**. Assume that b_1, b_2 are two such elements, and consider $a + b_1 + b_2$.

3. Find all the integral divisors of 105 and 125. How many are there in each case?

4. Write down the division with residue of 37 by 1, by 2, ... , by 10.

5. Write down the factorization into primes of 432, 1260, 5555.

6. Define a sequence by $F_0 = F_1 = 1$, and $F_{n+1} = F_{n-1} + F_n$. Prove that $(F_n, F_{n+1}) = 1$ for every n.

7. Prove that if $n \neq 3$ is a natural number, then $2^n > n^2$. **Hint**. Induction, but with care.

8. **a**. Prove that for every a, b, either $(a + b, a - b) = (a, b)$ or $(a+b, a-b) = 2(a, b)$. **b**. Prove that for every n, $(n^2+1, n+1) \in \{1, 2\}$.

$a + 0 = 0 + a = a$	neutral element
$\forall a \exists b \;\; a + b = 0$	inverse element
$a + b = b + a$	commutativity
$a + (b + c) = (a + b) + c$	associativity
$a \cdot 1 = 1 \cdot a = a$	neutral element
$ab = ba$	commutativity
$a(bc) = (ab)c$	associativity
$a(b + c) = ab + ac$	distributivity
For every a, b, either $a \leq b$ or $b \leq a$	linearity
$a \leq a$	irreflexivity
$a \leq b$ **and** $b \leq a \implies a = b$	antisymmetry
$a \leq b$ **and** $b \leq c \implies a \leq c$	transitivity
$a \leq b \implies a + c \leq b + c$	
$a \leq b$ **and** $0 \leq c \implies ac \leq bc$	

FIGURE 1. Axioms of $\mathbb{Z}$

Date: July 4, 2005.

.

Exercise Set 2. The greatest common divisor

1. Apply Euclid's algorithm to compute $(42, 34)$.
2. Apply Euclid's algorithm to compute $(216, 120)$.
3. Find *all* the pairs (a, b) (with $a \geq b \geq 0$) such that $(a, b) = 1$, and it takes the algorithm $n = 2$ to conclude this fact. **Hint**. First find all the pairs which are computed after $n = 0$ steps, and the pairs requiring $n = 1$ steps.
4. Let $[n, m]$ denote the minimal natural number divisible by n, m. Prove that $[n, m] \leq nm$.
5. Compute (directly from the definition) the numbers $[4, 6]$ and $[3, 7]$.
6. Without using the fundamental theorem, prove that $[n, m] = \frac{nm}{(n,m)}$. **Hint.** First prove that $\frac{nm}{(n,m)}$ is divisible by n, m, so that $[n, m] \leq \frac{nm}{(n,m)}$. Secondly show that if $n, m | g$, then also $\frac{nm}{(n,m)} | g$ (write $g = ng'$, $n = dn'$ and $m = dm'$ for $d = (n, m)$).
7. Prove that if $(a, b) = 1$, then $(n, ab) = (n, a)(n, b)$. **Hint.** Write $c = (n, a)$ and $d = (n, b)$, and notice that $(c, d) | (a, b) = 1$. Write $a = ca'$ and $b = db'$, then $(n/c, a') = (n/d, b') = 1$, and $(n, ab) = cd(n/(cd), a'b')$, but $(n/(cd), a') = (n/(cd), b') = 1$ (why?).
8. Prove that if $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ and $m = p_1^{\beta_1} \dots p_t^{\beta_t}$, then $[n, m] = p_1^{\max(\alpha_1, \beta_1)} \dots p_t^{\max(\alpha_t, \beta_t)}$.

Choose one of problems 6,7.

More exercises: a. Prove that $\frac{[a,b,c]}{(a,b,c)} = \frac{abc}{(a,b)(b,c)(c,a)}$.

b. Prove that $(an, bm) = (a, b)(n, m)(\frac{a}{(a,b)}, \frac{m}{(n,m)})(\frac{b}{(a,b)}, \frac{n}{(n,m)})$.

Exercise Set 3. Euclid's algorithm and modular computation

1. Apply the extended Euclid algorithm to find u, v such that $144u + 25v = 1$.
2. Apply the extended Euclid algorithm to find u, v such that $32u + 14v = 10$ (I know that 10 does not divide 32).
3. Prove that for every pair of integers n, m such that $7n + 5m = 1$, there exist some k such that $n = 5k - 2$ and $m = 3 - 7k$.
4. Find all the solutions $x \pmod{17}$ such that $6x \equiv 5 \pmod{17}$.
5. Recall that for every three numbers n, m, k, $(n, (m, k)) = ((n, m), k)$. Prove that this number is the greatest common divisor of n, m, k (so it makes sense to denote it as (n, m, k)).
6. Find example of numbers n, m such that $(n, m), (n, 63), (m, 63) > 1$, but yet $(n, m, 63) = 1$.
7. Prove that for every n, m, k, there always exist α, β, γ such that $\alpha n + \beta m + \gamma k = (n, m, k)$.
8. Find numbers a, b, c such that $77a + 91b + 143c = 1$.

Solution for exercise 7. Let $d = (n, m)$, and let r, s be integers such that $rn + sm = d$. By definition, $(n, m, k) = (d, k)$, so there are u, v such that $(n, m, k) = ud + vk = u(rn + sm) + vk = (ur)n + (us)m + (v)k$.

Exercise Set 4. Matrices, CRT, Newton's formula, Fermat's little theorem

1. Let $A = \begin{pmatrix} 1 & 2 \\ -3 & 2 \end{pmatrix}$. Compute the matrix A^8.
2. Let $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ and $C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$ be general matrices. Compute (and compare) the entry at the first row and second column of the products $(AB)C$ and $A(BC)$.
3. Find the only solution $\pmod{77}$ to the equations $x \equiv 2 \pmod 7$ and $x \equiv 3 \pmod{11}$.
4. Find the only solution $\pmod{385}$ to the equations $x \equiv 4 \pmod 7$, $x \equiv 6 \pmod{11}$ and $x \equiv 0 \pmod 5$.
5. Prove (either by induction, or otherwise) that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.
6. Prove that $\binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+m}{m} = \binom{n+m+1}{m}$ for any $n, m \geq 0$.
7. Compute $7^{205} \pmod{101}$.
8. Prove that $a^{12} \equiv 1 \pmod{1365}$ for every a which is prime to 1365. Check this statement for $a = 2$.

Exercise Set 5. Quadratic residues

1. Modulo 31, we have that $6^2 \equiv 5$, $8^2 \equiv 2$ and $11^2 \equiv -3$. Find the quadratic roots of -6 and 10.

2. Find the quadratic root of ± 7 modulo $p = 43$.

3. Suppose that $p \equiv -1 \pmod 8$ is a prime, and that $a \in U_p$ has a forth root modulo p (that is, $a \equiv c^4$ for some c). Let $b = a^{\frac{p+1}{8}}$. Prove that $b^4 \equiv a \pmod p$.

4. Let p be a prime, such that

$$\left(\frac{2}{p}\right) = +1, \left(\frac{3}{p}\right) = -1, \left(\frac{5}{p}\right) = -1, \left(\frac{7}{p}\right) = +1.$$

Compute the LaGrange symbols

$$\left(\frac{40}{p}\right), \left(\frac{42}{p}\right), \left(\frac{48}{p}\right), \left(\frac{49}{p}\right), \left(\frac{50}{p}\right).$$

5. Compute the following sums modulo the prime $p = 101$:

$$1 + 2 + \cdots + 100.$$
$$1^{50} + 2^{50} + \cdots + 100^{50}.$$
$$1^{51} + 2^{51} + \cdots + 100^{51},$$
$$1^{99} + 2^{99} + \cdots + 100^{99},$$
$$1^{100} + 2^{100} + \cdots + 100^{100},$$
$$1^{101} + 2^{101} + \cdots + 100^{101},$$

Exercise Set 6. U_n and orders of residues

1. Recall that a group is a set closed under multiplication (modulo some number n), in which every element has an inverse. Let d be an arbitrary integer.

a. Let $G^d = \{a^d : a \in U_n\}$ be the subset of elements which are d powers in $G = U_n$. Prove that G^d is a group.

b. Let $G_d = \{a \in U_n : a^d = 1\}$ be the subset of elements of order dividing d in $G = U_n$. Prove that G_d is a group.

2. Compute the sets G^4 and G_4 for the groups $G = U_8$, $G = U_{12}$ and $G = U_{18}$.

3. Let p be an odd prime, and $\alpha \geq 1$. Prove that there are only two solutions (modulo p^α) to the equation $x^2 \equiv 1 \pmod{p^\alpha}$.

4. Compute the sum $\sum_{d|24} \phi(d)$ by computing all the summands (and summing them up, of course).

5. Let $n = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. Compute the value of $\lambda(n)$, and find a number a such that $\mathrm{ord}_n(a) = \lambda(n)$ (notice: you only need to check that $a^{\lambda(n)/p} \not\equiv 1 \pmod{n}$ for all the prime factors of $\lambda(n)$).

6. Suppose that $p \equiv 1 \pmod 4$ is a prime. Show that there are precisely four different solutions to the equation $x^4 \equiv 1 \pmod{p}$.

7. Suppose that $e = \mathrm{ord}_n(a)$ is the order of a in U_n.

a. Let $d|e$ be any divisor. Prove that the order of a^d is e/d.

b. Let d be a number such that $(d, e) = 1$. Prove that the order of a^d is equal to e.

8. Find all the numbers n for which $\lambda(n) \leq 4$.

Exercise Set 7. Primality testing

1. Show that if p is a prime, then $2^p - 1$ is either a prime, or a strong pseudo-prime for the base $a = 2$.

2. Show that $3^n + 1$ is never divisible by 8.

3. Let $m \geq 3$. Prove that $a = 2^{m-1} \pm 1$ satisfy $a^2 \equiv 1 \pmod{2^m}$.

4. Prove that the equation $x^2 \equiv 1 \pmod{2^m}$ has precisely four solutions for every $m \geq 4$.

5. How many solutions are there to the equation $x^2 \equiv 1$ modulo $n = 168$? Prove your claim (without actually listing the solutions).

6. Given that $92^2 \equiv 51^2 \pmod{5863}$, factorize the number 5863.

7. You will need two different dice for this question. Roll the dice and write down the outcome, as an ordered pair of numbers from 1 to 6. Repeat this until you get the same result for the second time. How many times did you roll the dice? Repeat the whole experiment five times. Compare your average to the expected number $\sqrt{18\pi} + 2 \sim 9.5$.

8. Given that $332^2 + 99^2 = 188^2 + 291^2$, completely factorize the number $188^2 - 99^2$.

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