Lecture 6 : Divisibility and the Euclidean Algorithm

Yufei Zhao

July 24, 2007

1. If a and b are relatively prime integers, show that ab and $a+b$ are also relatively prime.
2. (a) If 2^n+1 is prime for some integer n, show that n is a power of 2.
   (b) If 2^n-1 is prime for some integer n, show that n is a prime.
3. Show that the fraction $\dfrac{12n+1}{30n+2}$ is irreducible for all positive integers n.
4. Let x, a, b be positive integers, show that $\gcd(x^a-1, x^b-1) = x^{\gcd(a,b)}-1$.
5. (a) Let p be a prime number. Determine the greatest power of p that divides $n!$, where n is a positive integer.
   (b) Let m and n be positive integers. Show that $\dfrac{(m+n)!}{m!n!}$ is an integer (without referring to binomial coefficients).
6. (USAMO 1972) Show that
$$\frac{\gcd(a,b,c)^2}{\gcd(a,b)\gcd(b,c)\gcd(c,a)} = \frac{\operatorname{lcm}(a,b,c)^2}{\operatorname{lcm}(a,b)\operatorname{lcm}(b,c)\operatorname{lcm}(c,a)}.$$
7. (a) Show that if a and b are relatively prime integers, then $\gcd(a+b, a^2-ab+b^2) = 1$ or 3.
   (b) Show that if a and b are relatively prime integers, and p is an odd prime, then
$$\gcd\left(a+b, \frac{a^p+b^p}{a+b}\right) = 1 \text{ or } p.$$
8. Let n be a positive integer.
   (a) Find n consecutive composite numbers.
   (b) Find n consecutive positive integers, none of which is a power of a prime.
9. Let $n > 1$ be a positive integer. Show that
$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$
is not an integer. (Try not to use any powerful results about the distribution of prime numbers.)

Problem Solving Session

July 24, 2007

1. Let a, b be positive integers. Show that $\gcd(a,b)\,\mathrm{lcm}(a,b) = ab$.
2. Let a, b, c be positive integers. Show that a divides bc if and only if $\frac{a}{\gcd(a,b)}$ divides c.
3. Show that the fraction $\dfrac{21n+4}{14n+3}$ is irreducible for all positive integers n.
4. Let n be a positive integer. Find $\gcd(n!+1, (n+1)!)$.
5. Find all positive integers d such that d divides both n^2+1 and $(n+1)^2+1$ for some integer n.
6. Let a and b be positive integers such that $a \mid b^2$, $b^2 \mid a^3$, $a^3 \mid b^4$, $b^4 \mid a^5$, ... Prove that $a = b$.
7. Let $n \geq 2$ and k be positive integers. Prove that $(n-1)^2 \mid (n^k - 1)$ if and only if $(n-1) \mid k$.
8. (AIME 1986) What is the largest positive integer n for which $n^3 + 100$ is divisible by $n + 10$?
9. Let m and n be positive integers. Show that $\dfrac{(2m)!(2n)!}{(m+n)!m!n!}$ is an integer.
10. Prove that $n^2 + 3n + 5$ can never be a multiple of 121 if n is a positive integer.
11. Let a and $b > 2$ be positive integers. Show that $2^a + 1$ is not divisible by $2^b - 1$.
12. Let $a, b, n > 1$ be positive integers. Show that $a^n + b^n$ is not divisible by $a^n - b^n$.
13. Prove that if $m > n$ then $a^{2^n} + 1$ is a divisor of $a^{2^m} - 1$. Show that if a, m, n are positive with $m \neq n$, then
$$\gcd(a^{2^m}+1, a^{2^n}+1) = \begin{cases} 1 & \text{if } a \text{ is even,} \\ 2 & \text{if } a \text{ is odd.} \end{cases}$$
14. Let $n > 1$ be a positive integer. Show that
$$1 + \frac{1}{3} + \frac{1}{5} + \cdots \frac{1}{2n-1}$$
is not an integer.

Lecture 7 : Fermat, Euler, and Wilson

Yufei Zhao

July 25, 2007

Notation: Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ denote the *complete residue system* mod n, and let $\mathbb{Z}_n^* = \{d \mid d \in \mathbb{Z}_n, \gcd(d, n) = 1\}$ denote the *reduced residue system* mod n.

1. **Fermat's little theorem.** Let p be a prime number.
   (a) Show that if k is an integer with $0 < k < p$, then $\binom{p}{k}$ is divisible by p.
   (b) Show that if $a \in \mathbb{Z}$, then $(a+1)^p \equiv a^p + 1 \pmod{p}$.
   (c) Show that if $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.
   (d) Show that if a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

2. Let a and m be relatively prime positive integers. Show that the following two sets are identical in mod m:
$$\{a, 2a, 3a, \ldots, (m-1)a\} \qquad \text{and} \qquad \{1, 2, 3, \ldots, m-1\}.$$

3. Let a and m be relatively prime positive integers. Show that there exists an integer x such that $ax \equiv 1 \pmod{m}$.
   We say that x is the *multiplicative inverse* (or just *inverse*) of a in mod m, denoted by a^{-1} when the context is clear.

4. **Another look at Fermat's little theorem.** Let p be a prime number, and a an integer not divisible by p.
   (a) Show that $\{a, 2a, 3a, \ldots, (p-1)a\} \equiv \{1, 2, 3, \ldots, p-1\} \pmod{p}$.
   (b) Show that $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}$.
   (c) Conclude that $a^{p-1} \equiv 1 \pmod{p}$.

5. **Euler's totient function.** We use $\phi(n)$ to denote the number of elements in $\{1, 2, \ldots, n\}$ that are relatively prime to n. That is, $\phi(n) = |\mathbb{Z}_n^*|$.
   (a) Compute $\phi(7)$ and $\phi(24)$.
   (b) Compute $\phi(p^n)$, where p is a prime and n is a positive integer.
   (c) Show that if m and n are relatively prime integers, then $\phi(mn) = \phi(m)\phi(n)$.
   (d) Find a formula for computing $\phi(n)$ in terms of the prime factorization of n.

6. **Euler's Theorem** Let a and m be relatively prime integers.
   (a) Let $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ be the set of positive integers less than m and relatively prime to m. Show that
$$\{r_1, r_2, \ldots, r_{\phi(n)}\} \equiv \{ar_1, ar_2, \ldots, ar_{\phi(n)}\} \pmod{m}.$$

(b) Show that $a^{\phi(m)} \equiv 1 \pmod{m}$.

7. **Wilson's Theorem** Let p be a prime number.

   (a) Show that the set of residues $\{2, 3, \ldots, p-2\}$ can be paired up into multiplicative inverses.

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

8. Let $p > 2$ be a prime number.

   (a) Suppose that $p \equiv 1 \pmod{4}$, show that $x^2 \equiv -1 \pmod{p}$ has a solution. (Hint: use Wilson's theorem)

   (b) Suppose that $x^2 \equiv -1 \pmod{p}$ has a solution, show that $p \equiv 1 \pmod{4}$. (Hint: use Fermat's little theorem.)

9. Let n be a positive integer. Show that all divisors of $4n^2 + 1$ have the form $4k + 1$ for some integer k.

Problem Solving Session

July 25, 2007

1. Let p be a prime number. If x is an integer, then show that $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

2. Let n be a positive integer. Show that if $(n-1)! \equiv -1 \pmod{n}$, then n is prime.

3. Let p, q be distinct prime numbers. Show that every integer a satisfies the congruence $a^{pq-p-q+2} \equiv a \pmod{pq}$.

4. **RSA public-key cryptography.** Alice and Bob are sending cryptic messages to each other. Let p and q be distinct primes and $n = pq$ and $t = (p-1)(q-1)$. Let e, d be positive integers such that $ed \equiv 1 \pmod{t}$. Alice takes a message, M (an integer relatively prime to n, and sends $C = M^e$ to Bob. Bob receives C and computes $M' = C^d \pmod{n}$. Prove that $M \equiv M' \pmod{n}$.

5. Let m be an even positive integer. Assume that

$$\{a_1, a_2, \ldots, a_m\} \quad \text{and} \quad \{b_1, b_2, \ldots, b_m\}$$

are two complete sets of residue classes modulo m. Prove that

$$\{a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m\}$$

is not a set of complete residue classes.

6. Let $p \geq 3$ be a prime, and let

$$\{a_1, a_2, \ldots, a_p\} \quad \text{and} \quad \{b_1, b_2, \ldots, b_p\}$$

be two sets of complete residue classes modulo p. Prove that

$$\{a_1 b_1, a_2 b_2, \ldots, a_p b_p\}$$

is not a complete set of residue classes modulo p.

7. Find all non-negative integer solutions to $4ab - a - b = c^2$.

8. For an odd positive integer $n > 1$, let S be the set of integers x, $1 \leq x \leq n$, such that both x and $x + 1$ are relatively prime to n. Show that $\prod_{x \in S} x \equiv 1 \pmod{n}$.

Lecture 8 : Residue Classes

Yufei Zhao

July 26, 2007

1. **Wilson's Theorem.** Let p be a prime number.
   (a) Show that the set of residues $\{2, 3, \ldots, p-2\}$ can be paired up into multiplicative inverses.
   (b) Show that $(p-1)! \equiv -1 \pmod{p}$.

2. Let $p > 2$ be a prime number.
   (a) Suppose that $p \equiv 1 \pmod{4}$, show that $x^2 \equiv -1 \pmod{p}$ has a solution.
   (Hint: use Wilson's theorem)
   (b) Suppose that $x^2 \equiv -1 \pmod{p}$ has a solution, show that $p \equiv 1 \pmod{4}$.
   (Hint: use Fermat's little theorem.)

3. Let n be a positive integer. Show that all divisors of $4n^2 + 1$ have the form $4k + 1$ for some integer k.

4. **Chinese remainder theorem**
   (a) If m and n are relatively prime integers greater than one, and a and b are arbitrary integers, then show that there exists an integer x such that

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

   (b) If $m_1, m_2, \ldots, m_k$ are pairwise relatively prime integers greater than one, and $a_1, a_2, \ldots, a_k$ are arbitrary integers, then show that there exists an integer x such that

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \ldots, k.$$

5. **Euler's totient function.** We use $\phi(n)$ to denote the number of elements in $\{1, 2, \ldots, n\}$ that are relatively prime to n. That is, $\phi(n) = |\mathbb{Z}_n^*|$.
   (a) Compute $\phi(7)$ and $\phi(24)$.
   (b) Compute $\phi(p^n)$, where p is a prime and n is a positive integer.
   (c) Show that if m and n are relatively prime integers, then $\phi(mn) = \phi(m)\phi(n)$.
   (d) Find a formula for computing $\phi(n)$ in terms of the prime factorization of n.

6. (a) Let p be a prime such that $p = x^2 + y^2$ for some integers x and y. Show that $p = 2$ or $p \equiv 1 \pmod{4}$.
   (b) Let p be a prime such that $p \equiv 1 \pmod{4}$. Then there exist positive integers x and y such that $p = x^2 + y^2$.
   (Hint: let a be an integer such that $a^2 \equiv -1 \pmod{p}$, and then consider the set of integers of the form $ax - y$, where $0 \le x, y < \sqrt{p}$. Use the pigeonhole principle.)

Problem Solving Session

July 26, 2007

1. Let n be a positive integer. Find $\gcd(n! + 1, (n + 1)!)$.

2. Let x, y be integers. Show that $2x + 3y$ is divisible by 7 if and only if $5x + 4y$ is divisible by 7.

3. Let $p \geq 3$ be a prime, and let

$$\{a_1, a_2, \ldots, a_p\} \quad \text{and} \quad \{b_1, b_2, \ldots, b_p\}$$

be two sets of complete residue classes modulo p. Prove that

$$\{a_1 b_1, a_2 b_2, \ldots, a_p b_p\}$$

is not a complete set of residue classes modulo p.

4. Find all non-negative integer solutions to $4ab - a - b = c^2$.

5. For any prime p, if $a^p \equiv b^p \pmod{p}$, prove that $a^p \equiv b^p \pmod{p^2}$.

6. Let p be a prime number, and suppose that a is an integer such that $a^2 \equiv -2 \pmod{p}$. Show that at least one of the equations $x^2 + 2y^2 = p$, $x^2 + 2y^2 = 2p$ has a solution.

7. For an odd positive integer $n > 1$, let S be the set of integers x, $1 \leq x \leq n$, such that both x and $x + 1$ are relatively prime to n. Show that $\prod_{x \in S} x \equiv 1 \pmod{n}$.

Lecture 9 : Equations and Polynomials

Yufei Zhao

July 27, 2007

1. (a) Let p be a prime such that $p = x^2 + y^2$ for some integers x and y. Show that $p = 2$ or $p \equiv 1 \pmod 4$.

   (b) Let p be a prime such that $p \equiv 1 \pmod 4$. Then there exist positive integers x and y such that $p = x^2 + y^2$.

   (Hint: let a be an integer such that $a^2 \equiv -1 \pmod p$, and then consider the set of integers of the form $ax - y$, where $0 \le x, y < \sqrt{p}$. Use the pigeonhole principle.)

2. Show that $15x^2 - 7y^2 = 9$ has no integer solutions.

3. Show that the only integer solution to

$$x^2 + y^2 + z^2 = 2xyz$$

   is $x = y = z = 0$.

4. Let p be a prime number. Let $f(x)$ be a polynomial with integer coefficients, such that the leading coefficient of f is nonzero. Prove that $f(x) \equiv 0 \pmod p$ has at most $\deg f$ solutions modulos p.

5. Let p be a prime number.

   (a) Show that all the coefficients of the polynomial

$$(x+1)(x+2)\cdots(x+p-1) - x^{p-1} + 1$$

   are divisible by p.

   (b) For all positive integers i, let σ_i denote the sum of the products of $1, 2, \ldots, p-1$ taken i at a time. For example, $\sigma_1 = 1 + 2 + \cdots + (p-1)$, $\sigma_2 = \sum_{1 \le i < j \le p-1} ij$. Show that $\sigma_1, \sigma_2, \ldots, \sigma_{p-2}$ are all divisible by p.

   (c) Prove Wilson's Theorem: $(p-1)! \equiv -1 \pmod p$.

6. **Wolstenholme's theorem.** Let $p > 3$ be a prime number.

   (a) Show that the numerator of $1 + \dfrac{1}{2^2} + \dfrac{1}{3^2} + \cdots + \dfrac{1}{(p-1)^2}$ is divisible by p.

   (b) Show that the numerator of $1 + \dfrac{1}{2} + \dfrac{1}{3} + \cdots + \dfrac{1}{(p-1)}$ is divisible by p^2.

Problem Solving Session

July 27, 2007

1. Prove that the only solution in rational numbers of the equation

$$x^3 + 3y^3 + 9z^3 - 9xyz = 0$$

is $x = y = z = 0$.

2. Find all triples of integers (x, y, z) such that

$$x^2 + y^2 + z^2 = 2007.$$

3. Find all integer solutions to $x^2 + y^2 + z^2 = 7w^2$.

4. Let p be a prime number, and suppose that there exists an integer a such that $a^2 \equiv -2 \pmod{p}$. Show that at least one of the equations $x^2 + 2y^2 = p$, $x^2 + 2y^2 = 2p$ has a solution.

5. Let n be a positive integer. Show that there exist integers x and y such that $n = x^2 + y^2$ if and only if each prime factor of n of the form $4k + 3$ appears an even number of times.

6. Let $p \geq 5$ be a prime number. Show that $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$.

7. (APMO 2006) Let $p \geq 5$ be a prime and let r be the number of ways of placing p checkers on a $p \times p$ checkerboard so that not all checkers are in the same row (but they may all be in the same column). Show that r is divisible by p^5. Here, we assume that all the checkers are identical.

Lecture 10 : Order of an Element

Yufei Zhao

July 28, 2007

1. Let $m > 1$ be a positive integer, and let a be an integer relatively prime to m. Show that there is a least positive integer d for which $a^d \equiv 1 \pmod{m}$.

   We say that d is the *order* of a modulo m, denoted by $\text{ord}_m(a)$ or simply $\text{ord}(a)$ is the modulus m is understood.

2. Let m be a positive integer, and a an integer relatively prime to m.

   (a) Show that $a^n \equiv 1 \pmod{m}$ if and only if $\text{ord}_m(a) \mid n$.

   (b) Furthermore, show that $a^{n_0} \equiv a^{n_1} \pmod{m}$ if and only if $\text{ord}_m(a) \mid n_0 - n_1$.

   (c) Show that $\text{ord}_m(a) \mid \phi(m)$.

3. Show that the order of 2 modulo 101 is 100.

4. Prove that for all positive integers $a > 1$ and n, we have $n \mid \phi(a^n - 1)$.

5. Prove that if p is a prime, then every prime divisor of $2^p - 1$ is greater than p.

6. Prove that if p is a prime, then $p^p - 1$ has a prime factor of the form $kp + 1$.

Evaluation Test 2

Yufei Zhao

July 28, 2007

1. (a) [**3**] State Fermat's little theorem.
   (b) [**7**] Prove Fermat's little theorem.

2. [**10**] Show that if a and b are relatively prime positive integers, then there exist integers m and n such that $a^m + b^n \equiv 1 \pmod{ab}$.

3. [**10**] Let a and $b > 2$ be positive integers. Show that $2^a + 1$ is not divisible by $2^b - 1$.

4. [**10**] Show that for every prime number p, we can find some positive integer n so that

$$2^n + 3^n + 6^n - 1$$

   is divisible by p.

Evaluation Test 2

Solutions

Yufei Zhao

July 28, 2007

1. (a) [**3**] State Fermat's little theorem.

   Solution: If p is a prime number, and a is an integer not divisible by p, then

   $$a^{p-1} \equiv 1 \pmod{p}.$$

   (b) [**7**] Prove Fermat's little theorem.

   Solution: Consider the two sets

   $$\{1, 2, 3, \ldots, p-1\} \quad \text{and} \quad \{a, 2a, 3a, \ldots, (p-1)a\}.$$

   We claim that the elements in the second set are simply a permutation of the elements in the first set. This is because no two i, j gets taken to the same residue when multiplied by a, as $ia \equiv ja$ implies that $p \mid (i-j)a$, which implies that $p|i-j$, which implies that $i = j$ (as $1 \le i, j < p$). Furthermore, none of the elements in the second set is divisible by p. Since there are only $p-1$ nonzero residues in mod p, the second set must then be the same as the first set.

   Then, by multiplying together all the elements in each set, we obtain that

   $$1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \equiv a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots (p-1) \cdot a^{p-1} \pmod{p}.$$

   Since $1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$ is not divisible by p, it follows that $a^{p-1} \equiv 1 \pmod{p}$.

   Alternate solution: We will prove that $a^p \equiv a$ for all $a \in \{0, 1, 2, \ldots, p-1\}$ by induction on a. For $a = 0$, the result is clear. Assume $a^p \equiv a \pmod{p}$. Then

   $$(a+1)^p = a^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$

   Here we used the fact that $\binom{p}{k}$ is divisible by p for $1 \le k \le p-1$ (this is true since in the expansion $\binom{p}{k} = \frac{p!}{(p-k)!k!}$, the factor p in the numerator cannot get canceled by any factors in the denominator). Therefore, $a^p \equiv a \pmod{p}$ implies that $(a+1)^p \equiv a+1$, and the induction is complete.

   Since $a^p \equiv a \pmod{p}$ is true for all residue classes mod p, it must be true for all integers a. Furthermore, if a is not divisible by p, then $a^p \equiv a \pmod{p}$ implies that $a^{p-1} \equiv 1$, as desired.

2. [**10**] Show that if a and b are relatively prime positive integers, then there exist integers m and n such that $a^m + b^n \equiv 1 \pmod{ab}$.

   Solution: Set $m = \phi(b)$ and $n = \phi(a)$. Then $a^m \equiv 1 \pmod{b}$ and $b^n \equiv 1 \pmod{a}$ by Euler' theorem. It follows that $a^m + b^n - 1$ is divisible by both a and b, and so it's divisible by ab (since a and b are relatively prime). Therefore, $a^m + b^n \equiv 1 \pmod{ab}$.

3. [**10**] Let a and $b > 2$ be positive integers. Show that $2^a + 1$ is not divisible by $2^b - 1$.

   Solution: Suppose that there exists such a pair a, b so that $2^a + 1$ is divisible by $2^b - 1$. Let $a = qb + r$, where q, r are integers and $0 \leq r < b$. Note that $2^b \equiv 1 \pmod{2^b - 1}$. So

   $$2^a + 1 = 2^{qb+r} + 1 = (2^b)^q \cdot 2^r + 1 \equiv (1)^q \cdot 2^r + 1 = 2^r + 1 \pmod{2^b - 1}.$$

   It follows that $2^b - 1$ divides $2^r + 1$, so $2^b - 1 \leq 2^r + 1$. However, since $r < b$, we have $2^r + 1 \leq 2^{b-1} + 1$. Combining the two inequalities, we get $2^b - 1 \leq 2^{b-1} + 1$, and thus $2^{b-1} \leq 2$, so $b \leq 2$, which contradicts the hypothesis that $b > 2$.

4. [**10**] Show that for every prime number p, we can find some positive integer n so that

   $$2^n + 3^n + 6^n - 1$$

   is divisible by p.

   Solution: If $p = 2$ or $p = 3$, then we can choose $n = 2$.

   Otherwise, choose $n = p - 2$. Since none of $2, 3, 6$ is divisible by p, using Fermat's little theorem, we have

   $$6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1) = 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \equiv 3 + 2 + 1 - 6 = 0 \pmod{p}$$

   It follows that $6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1)$ is divisible by p, and therefore $2^{p-2} + 3^{p-2} + 6^{p-2} - 1$ is divisible by p.

   Remarks: This problem is related to the identity $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 = 0$. Fermat's little theorem tells us that the inverse of an element can be found by $a^{-1} \equiv a^{p-2} \pmod{p}$.