Notes on Number Theory

Leung W.C.

April 23, 2015

Contents

1 Divisibility

1.1 Notation and concept of divisibility

To denote "a is divisible by b" mathematically, we write $b \mid a$. This is read as "b divides a". We can also say "b is a **divisor/factor** of a", or "a is a **multiple** of b".

Similarly, $b \nmid a$ means "b does not divide a".

We define $b \mid a$ as follows: let a, b be integers. If there exists some integer x that $a = bx$, then we have $b \mid a$. Some people add an additional constraint $b \neq 0$ in the definition. (*Note: the number 0 is divisible by all integers.*)

1.2 Basic properties of divisibility

Here is some properties about divisibility:

(i) If $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ for all integers m , n (e.g. $a \mid b - 2c$) ;

(ii) If $a \mid b$ and $b \mid c$, then $a \mid c$;

(iii) If $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.

The proof of property (i) is given below. The rest is left for readers.

Let $b = xa$ and $c = ya$ for some integers x and y.

$\because mb + nc = m(xa) + n(ya) = (mx + ny)a$

$\therefore a \mid mb + nc$ for all integers m, n. $\square$

Exercise:

1. If $n \mid 4a + 5b$, $n \mid 2a + 3b$, prove that $n \mid b$.
2. Prove that if $a \mid b$ and $c \mid d$, then $ac \mid bd$.
3. Prove that
   (a) If $x^2 + ax + b = 0$ has an integral root $x_0 \neq 0$, then $x_0 \mid b$.
   (b) If $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ has an integral root $x_0 \neq 0$, then $x_0 \mid a_0$.

   (Note: the questions above are special cases of the *rational root theorem.*)
4. Prove that $15 \mid 2^{4n} - 1$ for all positive integers n.
5. If $3 \mid a + b$, prove that $9 \mid a^3 + b^3$.
6. Given $5 \mid n$ and $17 \mid n$, prove that $85 \mid n$.
7. If a, b, n are integers that $a \mid bn$, $ax + by = 1$ for some integers x, y, prove $a \mid n$.
8. Let m be an integer that $m > 1$. Given $m \mid (m - 1)! + 1$, prove that m is a prime number.

2 Greatest common divisor

If $m \mid a$ and $m \mid b$, then m is a **common divisor** of a and b.

The **greatest common divisor** (GCD) is the largest positive integer that divides the numbers, i.e. the largest common divisor. The greatest common divisor of a and b is denoted (a, b) or $\gcd(a, b)$. For example, $\gcd(8, 12) = 4$.

Numbers a and b are co-prime or relatively prime if $\gcd(a, b) = 1$. The **least common multiple** (LCM) of a and b, i.e. the smallest positive numbers that is divisible by both a and b, is denoted $[a, b]$ or $\operatorname{lcm}(a, b)$.

Note: a and b can be any integer, including zero and negative numbers.

Theorems related to GCD (proof is left to readers):

(i) $(a_1, a_2) = (-a_1, a_2)$

(ii) If $a_1 \mid a_2$, then $(a_1, a_2) = (a_1) = |a_1|$.
Or more generally, if $a_1 \mid a_j$ for $j = 2, \ldots, k$, then $(a_1, a_2, \ldots, a_k) = (a_1) = |a_1|$;

(iii) For any integer x, we have $(a_1, a_2) = (a_1, a_2, a_1 x)$.
Or more generally, we have $(a_1, a_2, \ldots, a_k) = (a_1, a_2, \ldots, a_k, a_1 x)$;

(iv) For any integer x, we have $(a_1, a_2) = (a_1, a_2 + a_1 x)$.
Or more generally, we have $(a_1, a_2, \ldots, a_k) = (a_1, a_2 + a_1 x, \ldots, a_k)$;

(v) If p is a prime number, then $(p, a_1) = \begin{cases} p \text{ if } p \mid a \\ 1 \text{ if } p \nmid a \end{cases}$;

(vi) If $m \mid (a_1, a_2, \ldots, a_k)$, then $m\left(\frac{a_1}{m}, \frac{a_2}{m}, \ldots, \frac{a_k}{m}\right) = (a_1, a_2, \ldots, a_k)$.

More theorems related to GCD (proof is left to readers):

(i) If c is a common multiple of $a_1, a_2, \ldots, a_k$, then $[a_1, a_2, \ldots, a_k] \mid c$;

(ii) If d is a common divisor of $a_1, a_2, \ldots, a_k$, then $d \mid [a_1, a_2, \ldots, a_k]$;

(iii) $m(a_1, a_2, \ldots, a_k) = (ma_1, ma_2, \ldots, ma_k)$;

(iv) $(a_1, a_2, a_3 \ldots, a_k) = ((a_1, a_2), a_3 \ldots, a_k)$;

(v) If $(m, a) = 1$, then $(m, ab) = (m, b)$;

(vi) If $(m, a) = 1$, $m \mid ab$, then $m \mid b$;

(vii) $[a, b](a, b) = ab$;

(viii) There exists integers $x_1, x_2, x_3, \ldots, x_k$ that $(a_1, \ldots, a_k) = a_1 x_1 + \cdots + a_k x_k$,
i.e. $(a_1, \ldots, a_k)$ can be expressed as an integral linear combination of $a_1, \ldots, a_k$.
(Note: it is impossible for $a_1 x_1 + \cdots + a_k x_k$ to form a smaller natural number.)

Example: Given a, b, c are intgers. Prove that if $(a,b) = (a,c)$, then $(a,b,c) = (a,b)$;

Solution: $(a,b,c) = ((a,b),c) = ((a,c),c) = (a,c,c) = (a,c) = (a,b)$

Alt. solution: We prove that $(a,b,c) \geq (a,b)$ and $(a,b,c) \leq (a,b)$. The part $(a,b,c) \geq (a,b)$ is given as follows:

Let $d = (a,b) = (a,c)$. Now we have $d \mid a$, $d \mid b$ and $d \mid c$, therefore d is a common divisor of a, b and c. Now $(a,b,c) \geq d = (a,b)$.

And the part $(a,b,c) \leq (a,b)$ is left to readers as an exercise.

Example: Prove that $(a^2, ab, b^2) = (a^2, b^2)$ for all integers a and b.;

Solution: Let $d = (a,b)$, $a = dm$, $b = dn$.

Now $(m,n) = \dfrac{(a,b)}{d} = 1$. And hence $(m,n^2) = 1$ and then $(m^2,n^2) = 1$.

Therefore $(a^2,b^2) = (d^2m^2, d^2n^2) = d^2(m^2,n^2) = d^2$.

Also, $(a^2,ab,b^2) = (a^2,ab,ab,b^2) = ((a^2,ab),(ab,b^2)) = (a(a,b),b(a,b))$
$= (a,b)(a,b) = d^2$.

Hence the given identity is proved.

Exercise:

1. Given a, b and c are integers. Determine and explain whether the following are true. (i.e. Give a proof for true, and a counter-example for false.)

   (a) If $(a,b) = (a,c)$, then $[a,b] = [a,c]$;

   (b) If $d \mid a$, $d \mid a^2 + b^2$, then $d \mid b$;

   (c) If $a^4 \mid b^3$, then $a \mid b$;

   (d) If $a^2 \mid b^3$, then $a \mid b$;

   (e) If $a^2 \mid b^2$, then $a \mid b$;

   (f) $ab \mid [a^2, b^2]$;

   (g) $[a^2, ab, b^2] = [a^2, b^2]$;

   (h) $(a,b,c) = ((a,b),(a,c))$;

   (i) If $d \mid a^2 + 1$, then $d \mid a^4 + 1$;

   (j) If $d \mid a^2 - 1$, then $d \mid a^4 - 1$.

2. Prove that $(a,b,c) \leq (a,b)$ for integers a, b and c.

3. Prove that $(a,b) \leq (a+b, a-b)$ for integers a and b.

4. Give four integers that their GCD is 1, but the GCDs of any three of the numbers are not 1.

5. (Putnam 2000) Prove that the expression $\dfrac{\gcd(m,n)}{n}\dbinom{n}{m}$ is an integer for all pairs of integers $n \geq m \geq 1$.

2.1 Euclidean algorithm

Besides listing all divisors and short division, **Euclidean algorithm** is an effective way to find the greatest common divisors. The algorithm is as follows (why does it work?):

$$(a, b) = (b, a \bmod b) \text{ for integers } a,\ b \text{ that } a \geq b$$

(*Note: $a \bmod b$ is the remainder of the division of a by b, i.e.* $a \bmod b = a - b\left\lfloor \frac{a}{b} \right\rfloor$)

Example: Find the GCD of 1234 and 567.

Solution: $(1234, 567) = (567, 100) = (100, 67) = (67, 33) = (33, 1) = (1, 0) = 1$

Example: Find the GCD of $2n - 1$ and $n - 2$, where n is an integer.

Solution: $(2n-1, n-2) = (2n-1-2(n-2), n-2) = (3, n-2) = \begin{cases} 3 \text{ if } 3 \mid n-2 \\ 1 \text{ if } 3 \nmid n-2 \end{cases}$

Exercise:

1. Evaluate the following (all unknowns are integers):

(a) $(240, 46)$
(b) $(30, 45, 84)$
(c) $(2t + 1, 2t - 1)$
(d) $(2n, 2(n + 1))$
(e) $(kn, k(n + 2))$
(f) $(n - 1, n^2 + n + 1)$

2.2 Extended Euclidean algorithm

Euclidean algorithm can be modified to calculate the coefficients m, n in the equation $(a, b) = ma + nb$. This is known as the **extended Euclidean algorithm**.

Example: Find the GCD of 46 and 240, and express the GCD as an integral linear combination of the given numbers.

Solution:

Division	Quotient	Remainder	$x(\times 240)$	$y(\times 46)$
—	—	240	1	0
$240 \div 46$	5	46	0	1
$46 \div 10$	4	10	$1 - 5(0) = 1$	$0 - 5(1) = -5$
$10 \div 6$	1	6	$0 - 4(1) = -4$	$1 - 4(-5) = 21$
$6 \div 40$	1	4	$-4 - 1(5) = -9$	$21 - 1(-26) = 47$
$4 \div 2$	2	2	$5 - 2(-9) = 23$	$-26 - 2(47) = -120$

Therefore, $(46, 240) = 2 = -9(240) + 47(46)$.

(Also, $2 = (-9 + 23k)(240) + (47 - 120k)(46)$ for any integer k.)

Example: (1st IMO (1959) #1)

Prove that the fraction $\dfrac{21n+4}{14n+3}$ is not reducible for every natural number n.

Solution: $(21n+4, 14n+3) = (7n+1, 14n+3) = (7n+1, 1) = 1$

$\therefore$ The fraction $\dfrac{21n+4}{14n+3}$ is not reducible for every natural number n.

Exercise:

1. Find the GCD of the following, and express the GCD as an integral linear combination of the given numbers:

   (a) 206 and 40; (b) 57 and 81; (c) 3456 and 1720.

2. Find the positive integer x having $(x, 36) = 6$ and $[x, 36] = 180$.

3. Find integers a, b having $a + b = 192$ and $[a, b] = 660$.
   (Jilin Junior Secondary Mathematics Contest 1989)

4. Given $(a, b) = 1$. Prove the following:

   (a) $(a + b, ab) = 1$;

   (b) $(a + b, a - b) = 1$ or 2;

   (c) $(a + b, a^2 + b^2 - ab) = 1$ or 3;

5. Prove that $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$ for all integers m, n.

3 Prime numbers

A **prime number** is a natural number having exactly two positive divisors, 1 and itself. Natural numbers greater than 1 which are not primes are **composite numbers**.

Exercise:

1. Given n is an integer greater than 1. Prove that there exists prime number p satisfying $p \mid n$.

2. Prove that there are infinitely many prime numbers. (Use the result of Q1.)

4 Fundamental theorem of arithmetic

The fundamental theorem of arithmetic is that every positive integer greater than 1 has a prime factorization, i.e. $a = p_1p_2\cdots p_n$, and the expression is unique if we do not consider the order of the primes in the expression $p_1p_2\cdots p_n$.

If we write down the primes in index notation, we obtain

$$a = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s} \text{ where } p_1 < p_2 < \cdots < p_s.$$

which is known as the **canonical representation** of a or the **standard form** of a.

With the prime factorization of numbers, we are able to have the following results:

1. Given $a = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ and $b = p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s}$, then we have
   (a) $(a, b) = p_1^{\delta_1}p_2^{\delta_2}\cdots p_s^{\delta_s}$, where $\delta_j = \min(\alpha_j, \beta_j)$ for $1 \le j \le s$.
   (b) $[a, b] = p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_s^{\gamma_s}$, where $\gamma_j = \max(\alpha_j, \beta_j)$ for $1 \le j \le s$.
2. If $(a, b) = 1$, $ab = c^k$, then there exists integers u, v that $a = u^k, b = v^k$.
3. Given $a = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, we have
   (a) Denote $\tau(a)$ (or $d(a)$) be the number of positive divisors of a.
   We have $\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_s + 1) = \tau(p_1^{\alpha_1})\tau(p_2^{\alpha_2})\cdots\tau(p_s^{\alpha_s})$;
   (b) Denote $\sigma(a)$ be the sum of positive divisors of a.
   We have $\sigma(a) = \dfrac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\cdots\dfrac{p_s^{\alpha_s+1} - 1}{p_s - 1} = \displaystyle\prod_{j=1}^{s}\frac{p_j^{\alpha_j+1} - 1}{p_j - 1} = \sigma(p_1^{\alpha_1})\cdots\sigma(p_s^{\alpha_s})$.
4. $\tau(1) = \sigma(1) = 1$. Note that 1 does not have a prime factorization.

Example: Find the number and the sum of positive divisors of 720.

Solution:

$\because 720 = 2^4 \cdot 3^2 \cdot 5$

$$\therefore \tau(720) = (4 + 1)(2 + 1)(1 + 1) = 30,$$

$$\sigma(720) = \frac{2^5 - 1}{2 - 1}\cdot\frac{3^3 - 1}{3 - 1}\cdot\frac{5^2 - 1}{5 - 1} = 31 \cdot 13 \cdot 6 = 2418.$$

Example: Find $\displaystyle\sum_{d|a}\frac{1}{d}$. (Note: d takes the values of all positive divisors of a.)

Solution: $\displaystyle\sum_{d|a}\frac{1}{d} = \sum_{d|a}\frac{1}{\frac{a}{d}} = \frac{1}{a}\sum_{d|a} d = \frac{1}{a}\sigma(a).$

Exercise:

1. Find the number of positive divisors of 1200.
2. Find the sum of the positive divisors of 60.
3. Find the least possible number n that $\tau(n) = 6$
4. Find all possible values of n that $\tau(n)$ is an odd number.
5. Prove that $(a, b, c)(ab, bc, ca) = (a, b)(b, c)(c, a)$.
6. Prove that $(a, [b, c]) = [(a, b), (a, c)]$.
7. Given $g \mid ab$, $g \mid cd$ and $g \mid ab + cd$, prove $g \mid ac$ and $g \mid bd$.
8. Given a, b, n are positive integers that $a > b$. Prove that if $n \mid a^n - b^n$, then $n \left| \dfrac{a^n - b^n}{a - b} \right.$.
9. Prove that $\displaystyle\prod_{d \mid n} d = n^{\frac{\tau(n)}{2}}$.
10. Prove that n is a prime number if and only if $\tau(n) = n + 1$.
11. (39th IMO(1998) #3) For any positive integer n, let $d(n)$ denote the number of positive divisors of n (including 1 and n itself). Determine all positive integers k such that $d(n^2)/d(n) = k$ for some n.
12. (38th IMO(1997) #5) Find all pairs (a, b) of integers a, $b \geq 1$ that satisfy the equation $a^{b^2} = b^a$.

5 Congruence Relation

For integers a, b, m, $m \neq 0$, if $m \mid (a-b)$, i.e. $a-b=km$ for some integer k, then a and b are congruent modulo m, written as $a \equiv b \pmod{m}$. Otherwise a and b are not congruent modulo m, written as $a \not\equiv b \pmod{m}$.

Note that $m \mid (a-b) \Leftrightarrow -m \mid (a-b)$, therefore $a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{(-m)}$. **For convenience, we always take m to be positive.**

The statement $a \equiv b \pmod{m}$ means a and b have the same remainder when they are divided by m. However, there are a few different definitions of remainders. Given $a = mq + r$, where m is the divisor, q is the quotient and r is the remainder, we can define r in a few ways:

- $0 \leq r < m$, i.e. r is the **least non-negative remainder**.

  In this case, we have $a \bmod b = a - b\left\lfloor \frac{a}{b} \right\rfloor$.
- $-m/2 < r \leq m/2$, i.e. r is the **absolute least remainder**.
- $1 \leq r < m$, i.e. r is the **least positive remainder**.
- $\begin{cases} 0 \leq r < m \text{ for } a \geq 0 \\ -m < r \leq 0 \text{ if } a < 0 \end{cases}$. This is how computers perform modulo operations.

Here are a few properties of congruence relations:

(i) If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$. (Note: subtraction is also okay, but division is not!)

(ii) If $a \equiv b \pmod{m}$, $f(x)$ is an integral polynomial function (i.e. $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where $a_0, a_1, \ldots, a_n$ are integers), then $f(a) \equiv f(b) \pmod{m}$.

(iii) If $a \equiv b \pmod{m}$, $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $g(x) = b_0 + b_1x + \cdots + b_nx^n$ are two integral polynomial functions, $a_j = b_j$ for $0 \leq j \leq n$, then we have $f(a) \equiv g(b) \pmod{m}$. Special case: $f(a) \equiv g(a) \pmod{m}$.

(If $a_j = b_j$ for $0 \leq j \leq n$, we can denote $f(x) \equiv g(x) \pmod{m}$.)

(iv) If $a \equiv b \pmod{m}$, $d \mid m$, then $a \equiv b \pmod{d}$.

(v) $a \equiv b \pmod{m}$ is equivalent to $ka \equiv kb \pmod{|k|m}$, where k is an integer.

(vi) $ka \equiv kb \pmod{m}$ is equivalent to $a \equiv b \pmod{\frac{m}{(k,m)}}$, where k is an integer.

(Special case: if $(k, m) = 1$, then $ka \equiv kb \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$.)

(vii) $a \equiv b \pmod{m_j}$ for $1 \leq j \leq n$, then $a \equiv b \pmod{[m_1, m_2, \ldots, m_j]}$.

Pitfalls: note that the following are NOT true:

- $\times$ If $a = b \pmod{m}$, $c = d \pmod{m}$, then $a^c = b^d \pmod{m}$.
- $\times$ If $ka = kb \pmod{m}$, $a = b \pmod{m}$ (true only if $(k, m) = 1$).

We also define the **inverse** of a number modulo m as follows:

If $(a, m) = 1$, $ac \equiv 1 \pmod{m}$, then c is an inverse of a modulo m. This is denoted as $a^{-1} \pmod{m}$ or a^{-1}. For example, we can find the inverses modulo 7 and 12 below:

$a \pmod 7$	1	2	3	4	5	6
$a^{-1} \pmod 7$	1	4	5	2	3	6

$a \pmod{12}$	1	5	7	11
$a^{-1} \pmod{12}$	1	5	7	11

Here are a few properties of inverses:

(i) If c_1 and c_2 are two inverses of a, then $c_1 \equiv c_2 \pmod{m}$;

(ii) $(a^{-1})^{-1} \equiv a \pmod{m}$;

(iii) $(a^{-1}, m) = 1$.

Example: Find the (least non-negative) remainder of 101^{11} divided by 11.

Solution: $101^{11} \equiv 2^{11} = (2^5)^2 \times 2 = 32^2 \times 2 \equiv (-1)^2 \times 2 = 2 \pmod{11}$

Example: Find the last two digits of 3^{406}.

Solution:

We have $3^2 = 9 \equiv 1 \pmod 4$. Therefore $3^{406} = (3^2)^{203} \equiv 1 \pmod 4$.

Also, $3^3 = 27 \equiv 2 \pmod{25}$, $3^4 = 3^3 \times 3 \equiv 2 \times 3 = 6 \pmod{25}$,
$3^{10} = 3^4 \times (3^3)^2 \equiv 6 \times 2^2 \equiv -1 \pmod{25}$, $3^{20} = (3^{10})^2 \equiv (-1)^2 = 1 \pmod{25}$

Therefore, $3^{406} = (3^{20})^{20} \times (3^3)^2 \equiv 1 \times 2^2 = 4 \pmod{25}$

Consider $3^{406} \equiv 1 \equiv 29 \pmod 4$, $3^{406} \equiv 4 \equiv 29 \pmod{25}$,
we have $3^{406} \equiv 29 \pmod{100}$

i.e. The unit digit is 9, and the tens digit is 2. (Alternatively, we can find the number modulo 100 directly, but the numbers are larger.)

Example: Given x, y are integers. Show that $x^2 + y^2 = 2011$ has no solution.

Solution: $2011 \equiv 3 \pmod 4$. However, $x^2 \equiv 0$ or $1 \pmod 4$ (why?), so it is impossible to have $x^2 + y^2 \equiv 3 \pmod 4$. Hence the given equation has no solution.

Exercise:

1. Find the least non-negative remainder of 2^{400} modulo 10.
2. Find the last two digits of 2^{1000} and $9^{9^{9^9}}$. (Hint: $9^{10} \equiv 1 \pmod{100}$)
3. Find the least non-negative remainder of $(13481^{56} - 77)^{28}$ divided by 111.
4. Prove that $70! \equiv 61! \pmod{71}$.
5. Find the least non-negative remainder of 2^{2^k} modulo 10, where $k \geq 2$.
6. Solve $\begin{cases} n \equiv 2 \pmod{3} \\ n \equiv 3 \pmod{4} \\ n \equiv 4 \pmod{5} \end{cases}$.
7. Given n is an integer. Prove the following. (You may choose to use or not to use congruence relations.)
   (a) $6 \mid n(n+1)(n+2)$;
   (b) $8 \mid n(n+1)(n+2)(n+3)$;
   (c) If $2 \nmid n$, then $8 \mid n^2 - 1$ and $24 \mid n(n^2-1)$;
   (d) $6 \mid n^3 - n$;
   (e) $30 \mid n^5 - n$;
   (f) $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is an integer.
8. Show that there are no integral solution to the following equations.
   (a) $x^2 - 2y^2 = 77$;
   (b) $x^2 - 3y^2 + 5z^2 = 0$.
9. (6th IMO (1964) #1)
   (a) Find all positive integers n for which $2^n - 1$ is divisible by 7;
   (b) Prove that there is no positive integers n for which $2^n + 1$ is divisible by 7.
10. Derive divisibility check algorithms for positive divisors below 100. Provide necessary proofs. For example, the divisibility of the number $\overline{a_n a_{n-1} \cdots a_1 a_0}$ by 7 can be determined by the following methods:
    (a) Find $n = \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \cdots$ and check if $7 \mid n$;
    (b) Use $f(\overline{a_n a_{n-1} \cdots a_1 a_0}) = \overline{a_n a_{n-1} \cdots a_1} - 2a_0$ and check if $7 \mid f$; (Apply f recursively.)
    (c) Use $g(\overline{a_n a_{n-1} \cdots a_1 a_0}) = 3a_n \cdot 10^{n-1} + \overline{a_{n-1} \cdots a_1 a_0}$ and check if $7 \mid g$.
11. Given p is a prime, x, k are integers, $k \geq 0$. Prove that $(1+x)^p \equiv 1 + x^p \pmod{p}$ and $(1+x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}$.
12. Find the possible values of m for the following:
    (a) $32 \equiv 11 \pmod{m}$;
    (b) $1000 \equiv -1 \pmod{m}$;
    (c) $2^8 \equiv 1 \pmod{m}$.

13. If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, find the maximum possible value of m in terms of a, b, c, and d.

14. Determine and explain whether the following are true.
(All unknowns are integers except otherwise stated.)

    (a) If $a^2 \equiv b^2 \pmod{m}$, then $a \equiv b \pmod{m}$;
    (b) If $a^2 \equiv b^2 \pmod{m}$, then $a \equiv b \pmod{m}$ or $a \equiv -b \pmod{m}$;
    (c) If $a \equiv b \pmod{m}$, then $a^2 \equiv b^2 \pmod{m^2}$;
    (d) If $a \equiv b \pmod{2}$, then $a^2 \equiv b^2 \pmod{2^2}$;
    (e) If p is an odd prime, $p \nmid a$, the necessary and sufficient conditions of $a^2 \equiv b^2 \pmod{p}$ is $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$ exclusively (exactly one of them is true);
    (f) Given $(a, m) = 1$, $k \geq 1$. If $a^k \equiv b^k \pmod{m}$ and $a^{k+1} \equiv b^{k+1} \pmod{m}$, then $a \equiv b \pmod{m}$.

15. Given p is a prime, $p \nmid a$, $k \geq 1$. Prove $n^2 \equiv an \pmod{p^k}$ if and only if $n \equiv 0 \pmod{p^k}$ and $n \equiv a \pmod{p^k}$.

16. Find all positive integers a, b, c that satisfy the following conditions: $a \equiv b \pmod{c}$, $b \equiv c \pmod{a}$, $c \equiv a \pmod{b}$.

17. (17th IMO (1975) #4) When 4444^{4444} is written in decimal notation, the sum of its digits is A. Let B be the sum of the digits of A. Find the sum of the digits of B. (A and B are written in decimal notation.)

18. (25th IMO (1984) #2) Find one pair of positive integers a and b such that:

    (i) $ab(a+b)$ is not divisible by 7;
    (ii) $(a+b)^7 - a^7 - b^7$ is divisible by 7^7.

    Justify your answers.

5.1 Residue systems

A set of m integers, no two of which are congruent modulo m, is called a **complete residue system modulo m**.

The set of integers $\{0, 1, \ldots, m-1\}$ is called the **least residue system modulo m**.

A set of integers $\{r_1, r_2, \ldots, r_t\}$ is a **reduced residue system modulo m** if

(i) $(r_j, m) = 1$ for all $1 \leq j \leq t$;

(ii) $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$;

(iii) Given $(a, m) = 1$, then $a \equiv r_k \pmod{m}$ for some integer k.

For example, for $m = 12$, a complete residue system is $\{0, 1, 2, \ldots, 11\}$, and a reduced residue system is $\{1, 5, 7, 11\}$.

(Note: Instead of checking of criterion (iii), we can check that the set has the same number of elements as a known reduced residue system. Why?)

Exercise:

1. Prove that if $(a,m)=1$, $\{r_1,r_2,\ldots,r_t\}$ is a reduced residue system modulo m, then $\{ar_1,ar_2,\ldots,ar_t\}$ is also a reduced residue system modulo m.

5.2 Euler's totient function

Euler's totient function, denoted as $\varphi(n)$, is the number of elements in a reduced residue system modulo n. (Note: $\varphi(1)=1$)

If n has a prime factorization $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, then we have

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right)$$

If $n=ab$, $(a,b)=1$, we have $\varphi(n)=\varphi(a)\varphi(b)$. Therefore, we have

$$\varphi(n)=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_s^{\alpha_s})$$

Example: Find $\varphi(576)$

Solution: $576=2^6 3^2$. Therefore $\varphi(576)=576\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=192$.

5.3 Fermat's little theorem

Fermat's little theorem states that

- If a is an integer, p is a prime, then $a^p\equiv a \pmod p$.
- Special case: if $p\nmid a$, then $a^{p-1}\equiv 1 \pmod p$.

5.4 Euler's theorem

Euler's theorem states that

- If $(a,n)=1$, then $a^{\varphi(n)}\equiv 1 \pmod n$, where $\varphi(n)$ is the Euler's totient function.
- Note that Fermat's little theorem is a special case of Euler's theorem.

Proof: Let a, n be integers that $(a,n)=1$, $\{r_1,r_2,\ldots,r_{\varphi(n)}\}$ be a reduced residue system modulo n, then $\{ar_1,ar_2,\ldots,ar_{\varphi(n)}\}$ is a reduced residue system modulo n.

Now we have

$$ar_1ar_2\cdots ar_{\varphi(n)}\equiv r_1r_2\cdots r_{\varphi(n)} \pmod n$$

Since $(r_j,n)=1$ for $1\le j\le n$, therefore we have

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

□

Exercise:

1. Given d is an integer, $d \geq 3$. Prove that for each d, there exists an infinite number of integers n satisfying $d \nmid \varphi(n)$.

2. Prove that

   (a) $\varphi(mn) = (m,n)\varphi([m,n])$;

   (b) $\varphi(mn)\varphi((m,n)) = (m,n)\varphi(m)\varphi(n)$;

   (c) If $(m,n) > 1$, then $\varphi(mn) > \varphi(m)\varphi(n)$.

3. Find all integers n that $\varphi(n) = 24$.

4. Find all integers n that $\varphi(n) = 2^6$.

5. Find all integers n that

   (a) $\varphi(n) = \varphi(2n)$ (b) $\varphi(2n) = \varphi(3n)$ (c) $\varphi(3n) = \varphi(4n)$

6. Given q is a rational number. Prove that for each q, there exist integers m, n that satisfy $q = \dfrac{\varphi(m)}{\varphi(n)}$.

7. Prove that for all integers k, there exists some integer n that $\varphi(n) = \varphi(n+k)$.

8. Find all integers n that satisfy $\varphi(n) \mid n$.

9. Prove that $\sum_{d|m} \varphi(d) = \sum_{d|m} \varphi(\frac{m}{d}) = m$.

10. Given p is a prime number. If $a^p \equiv b^p \pmod{p}$, prove that $a^p \equiv b^p \pmod{p^2}$.