Number Theory (18 pages; 12/11/24)

Contents

Note: Unless stated otherwise, it is assumed that any numbers referred to (such as a and b) are integers.

(A) Notation

(1) $a|b$: a divides b ($a \nmid b$: a doesn't divide b)

(2) $\gcd(a, b)$: greatest common divisor (or highest common factor) of a and b

(3) If a and b share no prime factors, then they are said to be 'relatively prime' or 'co-prime' (and $\gcd(a, b) = 1$)

(4) If we divide b into a and obtain $a = qb + r$, then:

a is the dividend

b is the divisor

q is the quotient

r is the remainder

(5) ∃: there exists

∀: for all

(B) Divisibility tests

(1) A number is divisible by 3 if the sum of its digits is divisible by 3.

(2) A number is divisible by 4 if the number formed by its last two digits is divisible by 4.

(3) A number is divisible by 9 if the sum of its digits is divisible by 9.

(4) The number with digits $abcd \ldots z$ is divisible by 11 if

$a - b + c - d + \cdots - z$ is divisible by 11

(5) Examples:

(a) $1358016 = 11 \times 123456$

and $1 - 3 + 5 - 8 + 0 - 1 + 6 = 0$

(b) $9182736453 = 11 \times 834794223$

and $9 - 1 + 8 - 2 + 7 - 3 + 6 - 4 + 5 - 3 = 22$

(C) Euclidean algorithm

(1.1) Division theorem (or 'algorithm')

This states that, if a & b are integers, with $b \neq 0$, then there is a unique pair of integers q & r such that

$a = qb + r$, where $0 \leq r < |b|$

(1.2) Examples

$a = 24, b = 40 \Rightarrow 24 = 0(40) + 24$

$a = 24, b = 15 \Rightarrow 24 = 1(15) + 9$

$a = 24, b = -15 \Rightarrow 24 = (-1)(-15) + 9$

$a = 24, b = -40 \Rightarrow 24 = 0(-40) + 24$

$a = -24, b = 40 \Rightarrow -24 = (-1)(40) + 16$

$a = -24, b = 15 \Rightarrow -24 = (-2)(15) + 6$

$a = -24, b = -15 \Rightarrow -24 = (2)(-15) + 6$

$a = -24, b = -40 \Rightarrow -24 = (1)(-40) + 16$

Note: If $a = 232$ & $b = 11$, then $232 = 21 \times 11 + 1$,

but if $a = -232$ & $b = 11$, then $-232 = -22 \times 11 + 10$

(2) Theorem (A): If c divides a & b, then c divides $au + bv$, for all integers u & v

(3) Lemma (B): If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$

Proof

By the theorem in (2), a common divisor of a & b is a divisor of $r = a - qb$, and is therefore a common divisor of b & r.

Also, a common divisor of b & r is a divisor of $a = qb + r$, and is therefore a common divisor of a & b.

Thus, the common divisors of a & b are the same as the common divisors of b & r, and hence $\gcd(a,b) = \gcd(b,r)$.

Alternative Method: See STEP/Pure Exercises/Integers Q7

(4.1) Euclidean algorithm

This applies the lemma in (3) repeatedly.

Without loss of generality, we need only consider $\gcd(a,b)$, where a & b are positive integers, and $a > b$

[If a (for example) is zero, then $\gcd(a,b) = b$;

where either a or b is negative (or both are), then

$\gcd(a,b) = \gcd(|a|,|b|)$;

if $a = b$, then $\gcd(a,b) = a$]

(4.2) Example: Find $\gcd(90, 84)$

$90 = 1(84) + 6$

$84 = 14(6)$

So $\gcd(90, 84) = \gcd(84, 6) = 6$

[Note that this is quicker than writing $90 = 2 \times 3^2 \times 5$

and $84 = 2^2 \times 3 \times 7$, and selecting the lowest powers of the prime factors: 2×3, and also quicker than comparing the multiples of 90 and 84.]

Note: A related result (that can be used in algorithms) is:

$\gcd(a,b) = \gcd(a-b,b)$, where $a > b$.

(5.1) Bezout's identity: If a and b are non-zero integers, then there exist integers p & q such that $\gcd(a, b) = pa + qb$

The Euclidean algorithm can be used to find p & q.

(5.2) Example: Let $a = 84$ & $b = 30$

Then $84 = 2(30) + 24$

$30 = 1(24) + 6$

$24 = 4(6)$

so that $\gcd(84, 30) = 6$

and, working backwards in the algorithm,

$6 = 30 - 1(24)$

$= 30 - 1(84 - 2(30))$

$= 3(30) - 1(84)$

ie $6 = 3(30) + (-1)(84)$

(6) $\gcd(a, b)$ is the smallest positive integer that can be written as a linear combination of a and b **(Result C)**

Proof

Suppose that $D = pa + qb$, where $D < d = \gcd(a, b)$

Then $d|a$ & $d|b$, so that $d|D$, which contradicts $D < d$.

(7) a and b are co-prime $\Leftrightarrow \exists$ integers such that $ax + by = 1$ **(Result D)**

Proof

(i) Bezout's identity means that

a and b are co-prime $\Rightarrow \exists$ integers such that $ax + by = 1$

(ii) If $ax + by = 1$, then a and b are co-prime (if $\gcd(a, b) = d \neq 1$, then $d|1$, which isn't possible, so there is a contradiction)

(D) Modular arithmetic

(1.1) Congruence

a is said to be congruent to b modulo m if a and b leave the same remainder when they are divided by m (m is usually positive)

This is written $a \equiv b \pmod{m}$

(sometimes referred to as modular congruence)

[m is referred to as the modulus]

(1.2) Examples

$9 \equiv 2 \pmod{7}$

$9 \equiv 16 \pmod{7}$

(2) $a \equiv b \pmod{m}$ if $m|(a - b)$ **(Result E)**

The **least residue** of $a \pmod{m}$ is the value b such that $a \equiv b \pmod{m}$, and $0 \leq b < m$. The least residue of a is just the remainder when a is divided by m.

(3) Properties of congruences

(i) $a \equiv 0 \pmod{m} \Leftrightarrow m|a$

(ii) $a \equiv a \pmod m$

(iii) If $a \equiv b \pmod m$, then $b \equiv a \pmod m$

(iv) If $a \equiv b \pmod m$, and $b \equiv c \pmod m$, then $a \equiv c \pmod m$

(4.1) Rules of modular arithmetic

Suppose that $a \equiv b \pmod m$ and $c \equiv d \pmod m$, and $m, n > 0$.

(i) $ka \equiv kb \pmod m$

(ii) $a + c \equiv b + d \pmod m$ and $a - c \equiv b - d \pmod m$

(iii) $ac \equiv bd \pmod m$

Proof

rtp (result to prove): $m|(ac - bd)$

$a \equiv b \pmod m \Rightarrow a - b = pm$

and $c \equiv d \pmod m \Rightarrow c - d = qm$

So $ac - bd = ac - (a - pm)(c - qm) = m(pc + qa - pqm)$

(iv) $a^n \equiv b^n \pmod m$ (this follows from (iii))

(4.2) Example: Find the remainder when 263^5 is divided by 9

Solution

$263 = 270 - 7 \equiv -7 \equiv 2 \pmod 9$

Hence $263^5 \equiv 2^5 = 32 \equiv 5 \pmod 9$

(4.3) Example: Find the last digit of 523^{42}

Solution

$523 \equiv 3 \pmod{10}$; hence $523^{42} \equiv 3^{42} = (3^2)^{21}$

Then, as $3^2 \equiv -1 \pmod{10}$, $(3^2)^{21} \equiv (-1)^{21} = -1$.

So $523^{42} \equiv -1 \equiv 9 \pmod{10}$, and this is the last digit

(4.4) Example: Find the remainder when 16^{241} is divided by 7

Solution

$16 \equiv 2 \pmod 7$, and so $16^{241} \equiv 2^{241} = 2^{3\times 80+1} = 2(2^3)^{80}$

and $2^3 \equiv 1$, so that $(2^3)^{80} \equiv 1^{80} = 1$,

and then $2(2^3)^{80} \equiv 2$

(E) Congruence equations

(1) The following is a standard result **(Result F):**

Consider the equation $ax \equiv b \pmod m$ (*)

with $a, b, m \in \mathbb{Z}$ and $m > 0$

Suppose that $\gcd(a, m) = d$.

(i) If $d \nmid b$, then (*) has no solutions.

(ii) If $d|b$, then (*) has d solutions $(\text{mod } m)$

Proof of (i): Suppose that (*) has a solution, so that

$ax - b = km$ for some x & k

Then $b = ax - km$

As $d|a$ and $d|m$, it follows that $d|b$, which contradicts the assumption that $d \nmid b$.

To explore (ii), consider the following example.

Example: To find solutions of $12x \equiv 18 \pmod{30}$

Here $\gcd(12, 30) = 6$ and $6|18$, so (from the result above) we expect there to be 6 solutions (mod 30).

First of all, we can establish that there will be at least one solution:

We want to find x & k such that $12x - 18 = 30k$

Dividing through by $\gcd(12, 30) = 6$, this gives

$2x - 3 = 5k$, and $\gcd(2, 5) = 1$

We can now use the earlier result that, if p and q are co-prime, then ∃ integers such that $pX + qY = 1$.

In this case, we can find X & Y such that $2X + 5Y = 1$.

Then our equation $2x - 3 = 5k$ can be rewritten as $2x - 5k = 3$,

and $2X + 5Y = 1$ can be rewritten as $2(3X) - 5(-3Y) = 3$,

giving $x = 3X$ and $k = -3Y$, and so at least one solution exists.

We can now see how there will be d solutions (mod m):

Suppose that we have found x & k such that $12x - 18 = 30k$

Then consider another solution $x' = x + \lambda$, so that

$12(x + \lambda) - 18 = 30k'$

As $12x - 18 = 30k$, this means that $12\lambda \equiv 0 \pmod{30}$.

This holds for the integer $\lambda = \frac{30}{6} = 5$, as $12\left(\frac{30}{6}\right) = (\frac{12}{6})(30)$, but no smaller integer, as 6 is the largest number that is a divisor of both 30 and 12 (making both $\frac{30}{6}$ and $\frac{12}{6}$ integers).

It also holds for multiples of 5, from 0 up to $6-1$, with subsequent multiples repeating the cycle (as $6(\frac{30}{6}) \equiv 0(\frac{30}{6})$ (mod 30), $7\left(\frac{30}{6}\right) = 30 + (\frac{30}{6}) \equiv 1\left(\frac{30}{6}\right)$ etc).

Thus there are 6 solutions (mod 30), and d (mod m) in the general case.

(2.1) Multiplicative inverses

A **multiplicative inverse** of a (mod m) is defined to be the integer p that satisfies $ap \equiv 1$ (mod m), where we can assume that $\gcd(a,m) = 1$.

[Suppose that $\gcd(a,m) = d$. Then $ap \equiv 1$ (mod m)$\Rightarrow$ $ap - 1 = \lambda m \Rightarrow ap - \lambda m = 1$, and as $d|a$ & $d|m$, it follows that $d|1$, which means that $d = 1$, as $d > 0$.]

By Bezout's identity, as $\gcd(a,m) = 1$, there exist integers p & q such that $ap + mq = 1$, and then $ap \equiv 1$ (mod m).

As already seen, the Euclidean algorithm can be used to find p & q.

(2.2) Example: Find a positive multiplicative inverse of 5 (mod 6).

We have to find an integer p that satisfies $5p \equiv 1$ (mod 6).

To do this we find p & q such that $5p + 6q = 1$:

Applying the Euclidean algorithm,

$6 = 1(5) + 1$

$5 = 5(1)$

so that $1 = 6 - 1(5)$; ie $5(-1) + 6(1) = 1$

and so $p = -1$

Thus $5(-1) \equiv 1 \pmod 6$, and hence $5(-1) + 5(6) \equiv 1 \pmod 6$,

so that $5(5) \equiv 1 \pmod 6$; ie the required multiplicative inverse is 5.

(3) To solve the congruence equation $ax \equiv b \pmod m$ (assuming that $\gcd(a, m)\,|b$), multiply both sides by the multiplicative inverse p of $a \pmod m$, to give $apx \equiv bp \pmod m$

Then $ap \equiv 1 \Rightarrow\ apx \equiv x$, so that $x \equiv bp$. **(Result G)**

(4.1) Cancelling in modular arithmetic

If $ka \equiv kb \pmod m$ and $gcd(k, m) = d$,

then $a \equiv b \pmod{\frac{m}{d}}$ **(Result H)**

Proof: $ka \equiv kb \pmod m \Rightarrow m|k(a - b)$

Then, as $gcd(k, m) = d$, the prime factors of m that make up d will divide k, but will not necessarily divide $(a - b)$. However, the remaining prime factors of m must divide $(a - b)$, as they don't divide k, and so it follows that $\frac{m}{d}\,|(a - b)$; ie $a \equiv b \pmod{\frac{m}{d}}$

(4.2) Example: Solve the congruence equation $3x \equiv 12 \pmod 6$

As $\gcd(3, 6) = 3$, we can write $x \equiv 4 \pmod 2$, so that

$x \equiv 0 \pmod 2$.

(4.3) Example: Solve the congruence equation $18x \equiv 12 \pmod{40}$

As $\gcd(6, 40) = 2$, we can write $3x \equiv 2 \pmod{\frac{40}{2}}$;

ie $3x \equiv 2 \pmod{20}$.

Note that $\gcd(a, m) = 1$ (writing the congruence equation in the form $ax \equiv b \pmod{m}$). Had this not been the case, there would only have been a solution if $\gcd(a, m)|b$, and then it would have been possible to cancel the equation further, as $\gcd(a, m)$ would divide a, b & m.

We can now find the multiplicative inverse of 3; ie the p that satisfies $3p \equiv 1 \pmod{20}$.

Using Bezout's identity, we find p & q such that $3p + 20q = 1$.

Applying the Euclidean algorithm,

$20 = 6(3) + 2$

$3 = 1(2) + 1$

$2 = 2(1)$

so that $1 = 3 - 1(2) = 3 - 1\big(20 - 6(3)\big) = 3(7) + 20(-1)$

and so $p = 7$

Thus $3(7) \equiv 1 \pmod{20}$.

Then, to tackle $3x \equiv 2 \pmod{20}$, we multiply both sides by the multiplicative inverse, to give $7(3x) \equiv 14 \pmod{20}$, and then by the earlier result this gives $x \equiv 14 \pmod{20}$.

As $\gcd(3, 20) = 1$, this is the only solution, by result (F).

(F) Fermat's Little theorem

(1) This states that, if p is a prime number and a is any integer, then $a^p \equiv a \pmod{p}$.

(2) If p isn't a factor of a (so that $\gcd(a, p) = 1$), a can be cancelled from both sides, with no effect on the modulus, to give:

$a^{p-1} \equiv 1 \pmod p$. [**Result I**]

(3) It follows that $a^{p-2}.a \equiv 1 \pmod p$, so that (when p isn't a factor of a) a^{p-2} is a multiplicative inverse of $a \pmod p$.

[**Result J**]

(4) Example: Find the remainder when 2^{403} is divided by 13.

Solution: By Fermat's Little theorem, $2^{12} \equiv 1 \pmod{13}$.

Noting that $403 = 33 \times 12 + 7$,

$(2^{12})^{33} \equiv 1^{33} = 1$

$\Rightarrow 2^{403} = 2^7(2^{12})^{33} \equiv 2^7 = 128 = 130 - 2 \equiv -2 \equiv 11 \pmod{13}$

(5) If $ax \equiv b \pmod p$, where p is prime, and if p isn't a factor of a,

then, by Result F, there is one solution for x.

Then $a^{p-1}x \equiv a^{p-2}b \pmod p$,

and as $a^{p-1} \equiv 1$, it follows that $a^{p-1}x \equiv x$,

so that $x \equiv a^{p-2}b \pmod p$ [**Result K]**

(6) Example: Solve $5x \equiv 8 \pmod{17}$

Solution

By Results J and K, 5^{15} is a multiplicative inverse of $5 \pmod{17}$ and $x \equiv 5^{15} \times 8 \pmod{17}$

Now, $5^2 = 25 \equiv 8 \pmod{17}$,

so that $5^4 \equiv 8^2 = 64 = 68 - 4 \equiv -4 \equiv 13 \pmod{17}$,

and then

$5^6 = 5^4 \times 5^2 \equiv 13 \times 8 = 104 = 6 \times 17 + 2 \equiv 2 \pmod{17}$,

so that $5^{12} \equiv 2^2 = 4 \pmod{17}$,

and $5^{15} \times 8 = 5^{12} \times 5^2 \times (5 \times 8) \equiv 4 \times 8 \times 6 = 192 \pmod{17}$,

and hence $x \equiv 5^{15} \times 8 \equiv 192 = 170 + 17 + 5 \equiv 5 \pmod{17}$.

(7) Example: Find the remainder when 12^{1000} is divided by 7.

Solution

By Fermat's Little theorem, $12^6 \equiv 1 \pmod 7$, as 12 is not divisible by 7.

Then, as $1000 = (6 \times 166) + 4$,

$12^{996} = (12^6)^{166} \equiv 1^{166} = 1 \pmod 7$.

Also, $12^2 = 144 \equiv 4 \pmod 7$

and so $12^4 \equiv 4^2 = 16 \equiv 2 \pmod 7$.

Hence $12^{1000} = 12^{996} \times 12^4 \equiv 1 \times 2 = 2 \pmod 7$.

Appendix 1: Summary of results (see also Appendix 2)

(1) Division theorem (or 'algorithm'):

If a & b are integers, with $b \neq 0$, then there is a unique pair of integers q & r such that $a = qb + r$, where $0 \leq r < |b|$

(2) (Theorem A) If c divides a & b, then c divides $au + bv$, for all integers u & v

(3) (Lemma B) If $a = qb + r$, then $\gcd(a, b) = \gcd\,(b, r)$

(4) Euclidean algorithm: The application of the lemma in (3) to produce $\gcd(a, b)$.

(5) Bezout's identity: If a and b are non-zero integers, then there exist integers p & q such that $\gcd(a, b) = pa + qb$

(The Euclidean algorithm can be used to find p & q.)

(6) (Result C) $\gcd(a, b)$ is the smallest positive integer that can be written as a linear combination of a and b

(7) (Result D) a and b are co-prime $\Leftrightarrow$ $\exists$ integers such that $ax + by = 1$

(8) (Result E) $a \equiv b \pmod{m}$ if $m|(a - b)$

(9) (Result F) Consider the equation $ax \equiv b \pmod{m}$ (*)

with $a, b, m \in \mathbb{Z}$ and $m > 0$

Suppose that $\gcd(a, m) = d$.

(i) If $d \nmid b$, then (*) has no solutions.

(ii) If $d|b$, then (*) has d solutions (mod m)

(10) (Result K) If $ax \equiv b$ (mod p), where p is prime, and if p isn't a factor of a, then $x \equiv a^{p-2}b$ (mod p)

Appendix 2: Summary of congruence devices

(1) eg $7^2 = 49 \equiv 1$ (mod 12), so $7^{96} = (7^2)^{48} \equiv 1^{48} = 1$ (mod 12)

(using a power of 7 that is congruent to 1)

Congruence to -1 can also be useful.

(2) Problems involving the last digit of a number can usually be tackled by considering congruence mod 10.

Using the device in (1), where we look for congruence to 1 or -1 (mod 10), note the following:

$3^2 = 9 \equiv -1$ (mod 10), so $3^{4n} \equiv (-1)^{2n} = 1$ (mod 10)

$7^2 = 49 \equiv -1$ (mod 10), so $7^{4n} \equiv (-1)^{2n} = 1$ (mod 10)

$11 \equiv 1$ (mod 10), so $11^n \equiv 1$ (mod 10)

[Note that powers of even numbers will never be congruent to 1 or -1 (mod 10).]

(3) If $a \equiv b$ (mod m) and $c \equiv d$ (mod m), and $m, n > 0$.

(i) $ka \equiv kb$ (mod m)

(ii) $a + c \equiv b + d$ (mod m) and $a - c \equiv b - d$ (mod m)

(iii) $ac \equiv bd$ (mod m)

Special case: If $b \equiv c$ (mod m), then $ab \equiv ac$ (mod m)

(iv) $a^n \equiv b^n$ (mod m) (this follows from (iii))

(4) A multiplicative inverse p of a (mod m) [so that $ap \equiv 1$ (mod m), where we can assume that $\gcd(a, m) = 1$] can be found by applying the Euclidean algorithm to find p & q such that $ap + mq = 1$.

(5) (Result G) To solve the congruence equation $ax \equiv b$ (mod m) (assuming that $\gcd(a, m)\,|b$), multiply both sides by the multiplicative inverse p of a (mod m), to give $apx \equiv bp$ (mod m)

Then $ap \equiv 1 \Rightarrow\ apx \equiv x$, so that $x \equiv bp$.

(6) (Result H) If $ka \equiv kb$ (mod m) and $gcd(k, m) = d$,

then $a \equiv b$ (mod $\frac{m}{d}$)

(7) Fermat's Little theorem: If p is a prime number and a is any integer, then $a^p \equiv a$ (mod p).

(8) If p isn't a factor of a, $a^{p-1} \equiv 1$ (mod p) [Result I].

(9) When p isn't a factor of a, a^{p-2} is a multiplicative inverse of a

[Result J].