# MA 17: HOW TO SOLVE IT
# HANDOUT 2*: ELEMENTARY NUMBER THEORY: FACTS AND PROOFS

**Instructor** Lingfu Zhang (lingfuz@caltech) **Office** Linde Hall 358
**TA** Rodion Zaytsev (rzaytsev2@caltech)

This note explains some number-theoretic facts. The proofs use integer arithmetic, induction, and basic polynomial identities. Primitive roots are considered modulo a prime.

### *1. Divisibility, primes and composites, quotient and remainder*

For integers $a \neq 0$ and $b$, we write $a \mid b$ and say that $a$ *divides* $b$ if $b = ak$ for some integer $k$. Then $a$ is a *divisor* of $b$, and $b$ is a *multiple* of $a$. For example, $3 \mid 12$ and $3 \mid 0$, but $5 \nmid 12$.

A *prime* is an integer $p > 1$ whose only positive divisors are 1 and $p$. The first few primes are $2, 3, 5, 7, 11, 13, 17, 19$. A *composite* is an integer $n > 1$ that can be written as $n = ab$ with $1 < a < n$ and $1 < b < n$. Every integer greater than 1 is either prime or composite. The integer 1 is neither.

For any integer $a$ and positive integer $b$, there are unique integers $q, r$ such that

$$a = qb + r, \qquad 0 \leq r < b.$$

The integers $q, r$ are the quotient and remainder.

### *2. Greatest common divisors, least common multiples, and coprimality*

For integers $a, b$ not both zero, $\gcd(a, b)$ is their largest positive common divisor, i.e., the largest positive number that divides both. Signs do not matter: $\gcd(a, b) = \gcd(|a|, |b|)$, and $\gcd(a, 0) = |a|$ for $a \neq 0$. We say that $a, b$ are *relatively prime*, or *coprime*, if $\gcd(a, b) = 1$. Neither integer needs to be prime: 8 and 15 are coprime.

For positive integers $a, b$, their *least common multiple* $\operatorname{lcm}(a, b)$ is the smallest positive integer divisible by both. It exists because $ab$ is a common multiple.

For example,

$$\gcd(12, 18) = 6, \qquad \operatorname{lcm}(12, 18) = 36.$$

*The Euclidean algorithm.* If $a = qb + r$, then $\gcd(a, b) = \gcd(r, b)$: the two pairs have exactly the same common divisors. For positive inputs, repeated division gives strictly decreasing positive remainders until a remainder is zero. The divisor in that final division is the gcd. For general inputs, first take absolute values; a zero input is covered by the formula above. For example,

$$84 = 2 \cdot 30 + 24, \qquad 30 = 24 + 6, \qquad 24 = 4 \cdot 6.$$

Thus $\gcd(84, 30) = 6$.

### *3. Bézout's identity*

*Bézout's identity.* If $a, b$ are integers not both zero and $d = \gcd(a, b)$, then there are integers $x, y$ such that

$$ax + by = d.$$

*Proof.* Among all positive integers of the form $ax + by$ with $x, y \in \mathbb{Z}$, choose the smallest, say $c = ax_0 + by_0$. Such a positive combination exists since at least one of $a, b$ is nonzero.

Divide $a$ by $c$: write $a = qc + r$ with $0 \leq r < c$. Then

$$r = a - qc = a(1 - qx_0) + b(-qy_0).$$

If $r > 0$, this would be a smaller positive linear combination, contradicting the choice of $c$. Therefore $r = 0$, so $c \mid a$. The same argument shows $c \mid b$.

Every common divisor of $a, b$ divides every integer linear combination, hence divides $c$. Thus $c$ is the greatest common divisor. □

*Coprime cancellation for divisibility.* If $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

*Proof.* Choose $x, y$ with $ax + by = 1$ and multiply by $c$:

$$c = acx + bcy.$$

Both terms on the right are divisible by $a$. □

### *4. Prime factorization*

*Euclid's lemma.* If $p$ is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

*Proof.* If $p \nmid a$, the only possible positive common divisor of $p, a$ is 1. Hence $\gcd(p, a) = 1$, and coprime cancellation gives $p \mid b$. □

Repeated application shows that a prime dividing a finite product must divide at least one factor.

*Fundamental theorem of arithmetic.* Every integer $n > 1$ has a prime factorization

$$n = p_1^{e_1} \cdots p_t^{e_t},$$

where the $p_i$ are distinct primes and the $e_i$ are positive integers. This factorization is unique up to rearranging the factors.

*Proof. Existence.* Use strong induction on $n$. If $n$ is prime, there is nothing to prove. Otherwise $n = ab$ with $1 < a, b < n$. By induction, both $a$ and $b$ are products of primes, so their product is too.

*Uniqueness.* Write two factorizations with repeated primes allowed:

$$n = p_1 \cdots p_r = q_1 \cdots q_s.$$

By Euclid's lemma, $p_1$ divides some $q_j$. Since both are prime, $p_1 = q_j$. Reorder the $q_j$, cancel this common factor, and repeat. Neither side can have primes left over after the other becomes 1, since a nonempty product of primes is greater than 1. Thus the factors agree, including their multiplicities. □

For example, $360 = 2^3 \cdot 3^2 \cdot 5$.

### *5. Prime exponents and formulas for the gcd and lcm*

For a prime $p$ and a positive integer $n$, let $v_p(n)$ be the exponent of $p$ in the prime factorization of $n$. Equivalently, it is the largest nonnegative integer $e$ for which $p^e \mid n$. In particular, $v_p(1) = 0$, and $v_p(n) = 0$ when $p \nmid n$.

Multiplying prime factorizations gives

$$v_p(ab) = v_p(a) + v_p(b).$$

It also gives the useful test

$$a \mid b \quad \Longleftrightarrow \quad v_p(a) \le v_p(b) \text{ for every prime } p \qquad (a, b > 0).$$

*Gcd and lcm formulas.* For positive integers $a, b$,

$$v_p(\gcd(a,b)) = \min\{v_p(a), v_p(b)\},$$
$$v_p(\operatorname{lcm}(a,b)) = \max\{v_p(a), v_p(b)\}.$$

*Proof.* A common divisor can contain at most the smaller exponent of each prime. Taking exactly those smaller exponents gives a common divisor divisible by every common divisor, hence the gcd. A common multiple must contain at least the larger exponent of each prime. Taking exactly those larger exponents gives a common multiple dividing every common multiple, hence the lcm. □

Since $\min(r, s) + \max(r, s) = r + s$, comparison of all prime exponents proves

$$\boxed{\gcd(a,b)\operatorname{lcm}(a,b) = ab.}$$

For example, $84 = 2^2 \cdot 3 \cdot 7$ and $30 = 2 \cdot 3 \cdot 5$ give a gcd of 6 and an lcm of 420. In particular, coprime positive integers satisfy $\operatorname{lcm}(a, b) = ab$.

*Squares.* A positive integer is a perfect square exactly when all its prime exponents are even. Consequently, if $a, b$ are coprime positive integers and $ab$ is a square, then $a$ and $b$ are each squares.

### *6. Congruences: arithmetic with remainders*

Fix an integer $m \ge 2$, called the *modulus*. For integers $a, b$, the notation

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

means $m \mid a-b$. Equivalently, $a, b$ have the same remainder upon division by $m$. For example, $17 \equiv 3 \pmod 7$ and $-1 \equiv 6 \pmod 7$. There are exactly $m$ residue classes, represented by $0, 1, \ldots, m-1$.

If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

$$a + c \equiv b + d, \qquad a - c \equiv b - d, \qquad ac \equiv bd \pmod{m}.$$

Repeated multiplication gives $a^k \equiv b^k \pmod m$ for every positive integer $k$.

*Remainders of squares.* Squares have only a few possible remainders modulo small integers:

| Modulus | Possible remainders of $a^2$ |
|---|---|
| 3 | $0, 1$ |
| 4 | $0, 1$ |
| 5 | $0, 1, 4$ |
| 8 | $0, 1, 4$ |

To check each row, square the residues $0, 1, \ldots, m-1$ and reduce modulo $m$; opposite residues have the same square. In particular, every odd square is 1 modulo 8: if $a = 2k+1$, then $a^2 = 4k(k+1)+1$, and $k(k+1)$ is even. These restrictions can rule out integer solutions to equations. For example,

$x^2 + y^2 \equiv 0 \pmod 3$ forces both $x$ and $y$ to be divisible by 3, since the only way to add two square remainders to obtain 0 modulo 3 is $0 + 0$.

### *7. Modular inverses, cancellation, and Fermat's little theorem*

An integer $u$ is an *inverse of $a$ modulo $m$* if $au \equiv 1 \pmod m$. Such an inverse exists exactly when $\gcd(a, m) = 1$.

*Proof.* If $\gcd(a, m) = 1$, Bézout gives $ax + my = 1$, so $x$ is an inverse. Conversely, if $au \equiv 1 \pmod m$, then $au - mv = 1$ for some integer $v$; every common divisor of $a, m$ divides 1, so the gcd is 1. □

*Cancellation.* If $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$, multiply by an inverse of $c$ to obtain $a \equiv b \pmod m$. An inverse is unique modulo $m$: if $au \equiv av \equiv 1$, the same cancellation gives $u \equiv v$. The notation $a^{-1}$ refers to this residue class, not to the real number $1/a$.

For example, $3^{-1} \equiv 5 \pmod 7$, since $3 \cdot 5 \equiv 1$. Hence $3x \equiv 5 \pmod 7$ is equivalent to $x \equiv 25 \equiv 4 \pmod 7$.

*When cancellation is not valid.* We have $2 \cdot 1 \equiv 2 \cdot 4 \pmod 6$, but $1 \not\equiv 4 \pmod 6$. In general, if $d = \gcd(c, m)$, then

$$ac \equiv bc \pmod m \quad \Longleftrightarrow \quad a \equiv b \pmod{m/d}.$$

Indeed, dividing the divisibility statement $m \mid c(a - b)$ by $d$ gives $(m/d) \mid (c/d)(a - b)$, and $c/d$ is coprime to $m/d$. If $m/d = 1$, the condition simply places no restriction on $a, b$.

*Fermat's little theorem.* Let $p$ be prime. If $p \nmid a$, then

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

Equivalently, $a^p \equiv a \pmod p$ for every integer $a$.

*Proof.* Consider the $p - 1$ numbers $a, 2a, \ldots, (p - 1)a$. None is 0 modulo $p$, by Euclid's lemma. Their residues are distinct: if $ia \equiv ja \pmod p$, we can cancel $a$ because $\gcd(a, p) = 1$, giving $i \equiv j$ and thus $i = j$ for $1 \le i, j \le p - 1$.

Consequently these numbers are a rearrangement of $1, 2, \ldots, p - 1$ modulo $p$. Multiplying all of them gives

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

None of $1, \ldots, p - 1$ is divisible by $p$, so Euclid's lemma shows that their product is not divisible by $p$. We may therefore cancel $(p - 1)!$, proving the theorem. Multiplication by $a$ gives the second form when $p \nmid a$; when $p \mid a$, both sides of that form are 0 modulo $p$. □

### *8. Multiplicative order and primitive roots*

Let $p$ be prime and $p \nmid a$. The *multiplicative order of $a$ modulo $p$*, denoted $\mathrm{ord}_p(a)$, is the smallest positive integer $d$ such that $a^d \equiv 1 \pmod p$. Such a $d$ exists by Fermat's little theorem.

*Order divides every return exponent.* If $d = \mathrm{ord}_p(a)$, then for every nonnegative integer $k$,

$$a^k \equiv 1 \pmod p \quad \Longleftrightarrow \quad d \mid k.$$

*Proof.* If $d \mid k$, take a power of $a^d \equiv 1$. Conversely, write $k = qd + r$ with $0 \le r < d$. Then $a^k \equiv a^r$. If $a^k \equiv 1$ and $r > 0$, the exponent $r$ contradicts the minimality of $d$. Thus $r = 0$. □

In particular, $\operatorname{ord}_p(a) \mid p-1$. Also, the residues

$$1, a, a^2, \ldots, a^{d-1}$$

are all distinct. An equality $a^i \equiv a^j$ with $0 \le i < j < d$ could be cancelled to give $a^{j-i} \equiv 1$, contradicting the definition of $d$. The powers repeat with period $d$.

*Example.* Modulo 7 the powers are

| $k$ | | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|---|
| $2^k$ | (mod 7) | 1 | 2 | 4 | 1 | 2 | 4 | 1 |
| $3^k$ | (mod 7) | 1 | 3 | 2 | 6 | 4 | 5 | 1 |

Thus $\operatorname{ord}_7(2) = 3$, whereas $\operatorname{ord}_7(3) = 6$.

An integer $g$ is a *primitive root modulo* $p$ if $p \nmid g$ and $\operatorname{ord}_p(g) = p-1$. Equivalently, its powers

$$1, g, g^2, \ldots, g^{p-2}$$

represent every nonzero residue modulo $p$ exactly once: they are $p-1$ distinct nonzero residues. For example, 3 is a primitive root modulo 7, but 2 is not.

The next two sections prove that a primitive root exists for every prime.

### *9. Two elementary lemmas for the existence proof*

*Lemma 1: a polynomial root bound.* Let $p$ be prime, and let

$$F(X) = c_d X^d + \cdots + c_1 X + c_0$$

have integer coefficients with $p \nmid c_d$. Then $F(x) \equiv 0 \pmod{p}$ has at most $d$ distinct residue classes of solutions.

The hypothesis $p \nmid c_d$ ensures that the degree remains $d$ after reducing coefficients modulo $p$. If every coefficient is divisible by $p$, the bound can fail: for example, $F(X) = pX$ has degree 1 but vanishes at all $p$ residues.

*Proof.* Induct on $d$. For $d = 0$, the polynomial is a constant not divisible by $p$, so there are no roots. Suppose $d \ge 1$. If there is no root, the result is immediate. Otherwise choose one, represented by an integer $a$.

For every $j \ge 1$, the identity

$$X^j - a^j = (X-a)(X^{j-1} + aX^{j-2} + \cdots + a^{j-1})$$

shows that $F(X) - F(a) = (X-a)Q(X)$ for a polynomial $Q$ with integer coefficients, degree $d-1$, and leading coefficient $c_d$. Since $F(a) \equiv 0 \pmod{p}$, we obtain

$$F(X) \equiv (X-a)Q(X) \pmod{p}.$$

If $b$ is a root not congruent to $a$, then

$$0 \equiv (b-a)Q(b) \pmod{p}.$$

Here $b-a$ is nonzero modulo the prime $p$, so it can be cancelled. Thus $Q(b) \equiv 0$. By induction, there are at most $d-1$ such other roots. Including $a$, there are at most $d$. □

For a composite modulus the root bound can fail: $X^2 - 1$ has four roots $1, 3, 5, 7$ modulo 8. The proof above uses primality precisely when it cancels $b-a$.

*Lemma 2: combining coprime orders.* Suppose $u, v$ have orders $r, s$ modulo a prime $p$, and $\gcd(r, s) = 1$. Then

$$\operatorname{ord}_p(uv) = rs.$$

*Proof.* First, $(uv)^{rs} \equiv 1 \pmod{p}$. Now suppose $(uv)^k \equiv 1$ for a positive integer $k$. Raise this congruence to the $s$-th power. Since $v^s \equiv 1$, we get $u^{ks} \equiv 1$, and hence $r \mid ks$. Coprimality gives $r \mid k$. Raising to the $r$-th power similarly gives $s \mid k$.

Because $r, s$ are coprime, their least common multiple is $rs$, so $rs \mid k$. Thus every positive exponent returning $uv$ to 1 is a multiple of $rs$, and $rs$ itself works. This is exactly the claim. □

### *10. Every prime has a primitive root*

*Theorem.* For every prime $p$, there is an integer $g$ with $\operatorname{ord}_p(g) = p - 1$.

*Idea.* Factor $p - 1$ into prime powers. First build a residue with each of those prime-power orders. Then multiply the residues together, using Lemma 2.

*Proof.* If $p = 2$, take $g = 1$, whose order is $1 = p - 1$. Now suppose $p > 2$, put $N = p - 1$, and write

$$N = q_1^{e_1} \cdots q_t^{e_t}$$

with distinct primes $q_i$ and positive integers $e_i$.

*Step 1: choose a residue that misses a smaller exponent.* Fix $i$. The polynomial $X^{N/q_i} - 1$ has degree $N/q_i < N$, and its leading coefficient is 1. By Lemma 1 it cannot vanish at all $N$ nonzero residues modulo $p$. We can therefore choose $a_i$ with $p \nmid a_i$ and

$$a_i^{N/q_i} \not\equiv 1 \pmod{p}.$$

*Step 2: obtain order exactly $q_i^{e_i}$.* Set

$$b_i = a_i^{N/q_i^{e_i}}.$$

Fermat's little theorem gives

$$b_i^{q_i^{e_i}} = a_i^N \equiv 1 \pmod{p},$$

whereas our choice of $a_i$ gives

$$b_i^{q_i^{e_i-1}} = a_i^{N/q_i} \not\equiv 1 \pmod{p}.$$

The order of $b_i$ consequently divides $q_i^{e_i}$ but does not divide $q_i^{e_i-1}$. Every divisor of a prime power $q_i^{e_i}$ is a power of $q_i$. The only possibility is

$$\operatorname{ord}_p(b_i) = q_i^{e_i}.$$

*Step 3: combine the orders.* The integers $q_1^{e_1}, \ldots, q_t^{e_t}$ are pairwise coprime. Lemma 2, applied repeatedly, shows that

$$g = b_1 \cdots b_t \quad \text{has order} \quad q_1^{e_1} \cdots q_t^{e_t} = N = p - 1.$$

Thus $g$ is a primitive root modulo $p$. □

*The construction modulo 7.* Here $N = 6 = 2 \cdot 3$. The computations $3^3 \equiv -1$ and $3^2 \equiv 2 \pmod{7}$ let us choose $a_1 = a_2 = 3$. The construction yields

$$b_1 = 3^{6/2} \equiv 6 \pmod{7}, \qquad b_2 = 3^{6/3} \equiv 2 \pmod{7}.$$

Then 6 has order 2, and 2 has order 3. Their product $6 \cdot 2 \equiv 5$ therefore has order 6. Thus 5 is a primitive root.