Week 4: Number Theory: Congruences, Orders, Valuations

Lecture notes · Thu Oct 15 / Fri Oct 16

Toolbox: six facts that do most of the work.

1. **Fermat and Euler.** If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$; for every a, $a^p \equiv a$. If $\gcd(a,n)=1$ then $a^{\varphi(n)} \equiv 1 \pmod n$, where $\varphi(p_1^{e_1}\cdots p_r^{e_r}) = \prod p_i^{e_i-1}(p_i-1)$. Consequence: exponents may be reduced modulo $\varphi(n)$ (never modulo n).
2. **Orders.** For $\gcd(a,n)=1$, $\mathrm{ord}_n(a)$ is the least $d \geq 1$ with $a^d \equiv 1 \pmod n$. Then $a^k \equiv 1 \pmod n \iff d \mid k$; in particular $d \mid \varphi(n)$, and $d \mid p-1$ when $n=p$. Workhorse corollaries: $2^a-1 \mid 2^b-1 \iff a \mid b$; $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)}-1$; every prime $q \mid a^p-1$ with p prime and $q \nmid a-1$ satisfies $q \equiv 1 \pmod p$. Primitive roots (elements of order $\varphi(n)$) exist modulo p, p^e, $2p^e$ for odd p, and modulo $2, 4$.
3. **Wilson.** $(p-1)! \equiv -1 \pmod p$ for p prime, since $2, \ldots, p-2$ pair off into inverses. Conversely $(n-1)! \equiv 0 \pmod n$ for composite $n > 4$.
4. **Chinese remainder theorem.** If $\gcd(m,n)=1$ then $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$ as rings. Work one prime power at a time and reassemble; φ and "$x \mapsto x^k$ is a bijection" are both computed this way.
5. **p-adic valuations.** $v_p(ab) = v_p(a) + v_p(b)$; $v_p(a+b) \geq \min(v_p(a), v_p(b))$ with *equality when* $v_p(a) \neq v_p(b)$. Legendre: $v_p(n!) = \sum_{k \geq 1} \lfloor n/p^k \rfloor = \frac{n - s_p(n)}{p-1}$, s_p the base-p digit sum. Lifting the exponent: if p is an odd prime, $p \mid x-y$, $p \nmid xy$, then $v_p(x^n - y^n) = v_p(x-y) + v_p(n)$.
6. **gcd tricks.** $\gcd(a,b) = \gcd(a, b-ka)$ (Euclid); $\gcd(a,b)=1$ and $a \mid bc$ imply $a \mid c$; coprime factors of a perfect power are perfect powers; and $xy + \alpha x + \beta y = c$ factors as $(x+\beta)(y+\alpha) = c + \alpha\beta$, turning a Diophantine equation into a divisor count.

Example 1 (The last two digits of 7^{2026})**.** *We want* $7^{2026} \bmod 100$. *Euler gives* $7^{40} \equiv 1 \pmod{100}$, *but the order is smaller:* $7^2 = 49$, $7^4 = 2401 \equiv 1 \pmod{100}$, *so* $\mathrm{ord}_{100}(7) = 4$. *Since* $2026 = 4 \cdot 506 + 2$, *we get* $7^{2026} \equiv 7^2 = 49$. *The last two digits are* 49. *Moral: compute the actual order when you can;* $\varphi(n)$ *is only an upper bound for it.*

Example 2 (Wilson, symmetrized)**.** For an odd prime p, $\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{(p+1)/2} \pmod p$. *Pair each* $k \in \{1, \ldots, \frac{p-1}{2}\}$ *with* $p-k \equiv -k$. *Then*

$$-1 \equiv (p-1)! = \prod_{k=1}^{(p-1)/2} k\,(p-k) \equiv \prod_{k=1}^{(p-1)/2} (-k^2) = (-1)^{(p-1)/2}\left(\tfrac{p-1}{2}\right)!^2 \pmod p.$$

Multiply by $(-1)^{(p-1)/2}$ *to finish. For* $p \equiv 1 \pmod 4$ *this exhibits a square root of* -1 *modulo* p, *namely* $\left(\frac{p-1}{2}\right)!$; *e.g.* $p = 13$: $6! = 720 = 55 \cdot 13 + 5$ *and* $5^2 = 25 \equiv -1$.

Example 3 (A valuation that cannot cancel)**.** For $n \geq 2$, $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ is not an integer. *Let* 2^k *be the largest power of* 2 *with* $2^k \leq n$, *so* $k \geq 1$. *Among* $1, \ldots, n$ *the only multiple of* 2^k *is* 2^k *itself (the next one,* 2^{k+1}, *exceeds* n*). Hence* $v_2(1/2^k) = -k$, *while every other term has* $v_2(1/j) = -v_2(j) > -k$. *A sum in which exactly one term has the minimum valuation has that valuation (the "equality when valuations differ" clause, applied repeatedly), so* $v_2(H_n) = -k < 0$ *and* $H_n \notin \mathbb{Z}$.

Pitfall. (1) Fermat needs $p \nmid a$ and Euler needs $\gcd(a, n) = 1$: $2^{\varphi(4)} = 4 \not\equiv 1 \pmod 4$. Use $a^p \equiv a$ when you cannot exclude $p \mid a$. (2) Exponents reduce modulo $\varphi(n)$ or modulo the order, never modulo n; bases reduce modulo n. (3) You may cancel c from $ca \equiv cb \pmod n$ only when $\gcd(c, n) = 1$; otherwise you get $a \equiv b \pmod{n/\gcd(c, n)}$. (4) $v_p(a + b) = \min(v_p(a), v_p(b))$ is a theorem only when the two valuations differ. (5) "$n \mid 2^n - 1$ forces $n = 1$" is proved with the *smallest* prime factor p of n (then $\gcd(n, p - 1) = 1$ kills the order); an arbitrary prime factor does not close the argument.

How to recognize this technique on the exam. Numbers that are absurdly large ("7^{2026}", "$n < 10^{100}$", the current year in an exponent) are an invitation to reduce modulo something and to compute an order. Statements of the form "find all n with $n \mid 2^n - 1$" or "every prime divisor of ... satisfies ..." are order arguments: name the order, note what it divides, and squeeze. A factorial, a binomial coefficient, or a claim that some expression is "never an integer" or "never a perfect square" asks for a valuation, usually at the prime 2 or the largest prime available. Equations in positive integers such as $1/a + 1/b = c/N$ want to be factored, after which the question is a divisor count with a congruence condition. Permutations of $\{1, \ldots, n\}$ defined by $k \mapsto mk \bmod n$ are the Chinese remainder theorem in disguise: split $\mathbb{Z}/n$ into prime-power pieces.

Suggested timing (15 minutes). 0–4: Fermat/Euler and orders; Example 1, stressing "order divides $\varphi(n)$" and the corollary $2^a - 1 \mid 2^b - 1 \iff a \mid b$. 4–8: Wilson via pairing inverses; Example 2. 8–12: valuations, Legendre's formula, Example 3. 12–15: CRT and the factoring trick in one line each; pitfalls (1) and (2); then groups start on Problems 1–4.