Week 4: Number Theory: Congruences, Orders, Valuations

Handout · Thu Oct 15 / Fri Oct 16

Fermat/Euler: $a^{p-1} \equiv 1 \pmod{p}$ for $p \nmid a$, and $a^{\varphi(n)} \equiv 1 \pmod{n}$ for $\gcd(a,n) = 1$; exponents reduce mod $\varphi(n)$, not mod n. **Orders:** if $d = \operatorname{ord}_n(a)$ then $a^k \equiv 1 \iff d \mid k$, so $d \mid \varphi(n)$; in particular $2^a - 1 \mid 2^b - 1 \iff a \mid b$, and any prime $q \mid 2^p - 1$ has $p \mid q-1$. **Wilson:** $(p-1)! \equiv -1 \pmod{p}$. **CRT:** $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$ for $\gcd(m,n) = 1$; work one prime power at a time. **Valuations:** $v_p(ab) = v_p(a) + v_p(b)$, $v_p(a+b) \geq \min$ with equality when $v_p(a) \neq v_p(b)$, and $v_p(n!) = \sum_{k\geq 1} \lfloor n/p^k \rfloor$. **gcd/factoring:** $\gcd(a,b) = \gcd(a, b-ka)$; $\gcd(a,b) = 1$ and $a \mid bc$ give $a \mid c$; $xy + \alpha x + \beta y = c$ is $(x+\beta)(y+\alpha) = c + \alpha\beta$.

Problem 1. $\star$ *(warm-up)* Show that 30 divides $n^5 - n$ for every integer n. Then show that 2730 divides $n^{13} - n$ for every integer n.

Problem 2. $\star$ *(warm-up)*

(a) Show that if $2^n - 1$ is prime, then n is prime.

(b) Let p be a prime and let q be a prime divisor of $2^p - 1$. Show that $q \equiv 1 \pmod{p}$. (In fact $q \equiv 1 \pmod{2p}$ when p is odd.)

(c) Use (b) to find, by hand and with almost no trial division, a prime factor of $2^{11} - 1 = 2047$.

Problem 3. $\star\star$ *(Putnam 2018 A1)* Find all ordered pairs (a,b) of positive integers for which

$$\frac{1}{a} + \frac{1}{b} = \frac{3}{2018}.$$

Problem 4. $\star\star$ *(Putnam 2016 A1)* Find the smallest positive integer j such that for every polynomial $p(x)$ with integer coefficients and for every integer k, the integer

$$p^{(j)}(k) = \left.\frac{d^j}{dx^j}\, p(x)\right|_{x=k}$$

(the j-th derivative of $p(x)$ at k) is divisible by 2016.

Problem 5. $\star\star\star$ *(Putnam 2018 B3)* Find all positive integers $n < 10^{100}$ for which simultaneously n divides 2^n, $n-1$ divides $2^n - 1$, and $n-2$ divides $2^n - 2$.

Problem 6. $\star\star\star\star$ *(Putnam 2023 B5)* Determine which positive integers n have the following property: for all integers m that are relatively prime to n, there exists a permutation $\pi\colon \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ such that $\pi(\pi(k)) \equiv mk \pmod{n}$ for all $k \in \{1,2,\dots,n\}$.

Problems 1–4 are the in-session targets; 5–6 are take-home. Solutions will be posted after Friday's session.