Week 4: Number Theory: Congruences, Orders, Valuations

Solutions · Thu Oct 15 / Fri Oct 16

Problem 1. ⋆ *(warm-up) Show that* $30 \mid n^5 - n$ *and* $2730 \mid n^{13} - n$ *for every integer* n.
Key idea. Check one prime at a time with Fermat's little theorem in the form $n^p \equiv n \pmod p$, then multiply, since distinct primes are coprime.

Solution. Factor $30 = 2 \cdot 3 \cdot 5$. Write $n^5 - n = (n-1)\,n\,(n+1)(n^2+1)$. Among the three consecutive integers $n-1, n, n+1$ one is even and one is a multiple of 3, so $6 \mid n^5 - n$. For the prime 5, Fermat's little theorem says $n^5 \equiv n \pmod 5$ for every integer n (if $5 \nmid n$ this is $n^4 \equiv 1$ multiplied by n; if $5 \mid n$ both sides are 0). Since $2, 3, 5$ are pairwise coprime and each divides $n^5 - n$, their product 30 does.

Now $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$, and for each of these primes p we have $p - 1 \in \{1, 2, 4, 6, 12\}$, a divisor of 12. Fix such a p. If $p \mid n$ then $n^{13} \equiv 0 \equiv n \pmod p$. If $p \nmid n$, Fermat gives $n^{p-1} \equiv 1$, hence $n^{12} = (n^{p-1})^{12/(p-1)} \equiv 1$ and $n^{13} \equiv n \pmod p$. So each of the five primes divides $n^{13} - n$, and, being pairwise coprime, so does their product 2730. □

Remark. The choice of 2730 is sharp: $n = 2$ gives $2^{13} - 2 = 8190 = 3 \cdot 2730$, and $n = 3$ gives $3^{13} - 3 = 1594320 = 584 \cdot 2730$ with $\gcd(3, 584) = 1$, so the greatest common divisor of all values $n^{13} - n$ is exactly 2730. In general $\gcd_n(n^k - n)$ is the product of the primes p with $p - 1 \mid k - 1$.

Problem 2. ⋆ *(warm-up) (a) If* $2^n - 1$ *is prime then* n *is prime. (b) If* p *is prime and* q *is a prime divisor of* $2^p - 1$*, then* $q \equiv 1 \pmod p$*. (c) Factor* $2^{11} - 1 = 2047$.
Key idea. The order of 2 modulo q divides both p and $q - 1$; a divisor of a prime is 1 or the prime.

Solution. (a) If $n = 1$ then $2^n - 1 = 1$ is not prime. If $n = ab$ with $1 < a < n$, put $x = 2^a$; then $2^n - 1 = x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + \cdots + 1)$, and $1 < 2^a - 1 < 2^n - 1$, so $2^n - 1$ has a proper divisor and is not prime. Hence $2^n - 1$ prime forces n prime.

(b) The number $2^p - 1$ is odd, so q is an odd prime and $\gcd(2, q) = 1$. Let $d = \operatorname{ord}_q(2)$, the least positive integer with $2^d \equiv 1 \pmod q$. From $q \mid 2^p - 1$ we get $2^p \equiv 1 \pmod q$, and the basic property of orders gives $d \mid p$. Since p is prime, $d \in \{1, p\}$; but $d = 1$ would mean $q \mid 2 - 1 = 1$, impossible. So $d = p$. By Fermat's little theorem $2^{q-1} \equiv 1 \pmod q$, so $d = p$ divides $q - 1$; that is, $q \equiv 1 \pmod p$. For p odd, $q - 1$ is also even, and $\gcd(2, p) = 1$ gives $2p \mid q - 1$.

(c) By (b) every prime factor of 2047 is $\equiv 1 \pmod{22}$. The integers $\equiv 1 \pmod{22}$ up to $\sqrt{2047} < 46$ are 23 and 45, and only 23 is prime. Indeed $2047 = 23 \cdot 89$, and $89 = 4 \cdot 22 + 1$ as predicted. □

Remark. Part (b) is how Euler showed that $2^{31} - 1$ is prime: the only possible prime factors are primes $\equiv 1 \pmod{62}$ below $\sqrt{2^{31}} < 46341$ (Euler also knew they must be $\equiv \pm 1 \pmod 8$), which reduces about 4800 trial divisions to 84.

Problem 3. ⋆⋆ *(Putnam 2018 A1) Find all ordered pairs* (a, b) *of positive integers with* $1/a + 1/b = 3/2018$.
Key idea. Clear denominators and factor: the equation becomes $(3a - 2018)(3b - 2018) = 2018^2$, and a congruence mod 3 picks out the admissible divisors.

Solution. Multiplying by $2018ab$ gives $2018(a + b) = 3ab$, i.e. $9ab - 3 \cdot 2018\,a - 3 \cdot 2018\,b = 0$. Adding 2018^2 to both sides completes the factorization:

$$(3a - 2018)(3b - 2018) = 2018^2.$$

Set $u = 3a - 2018$, $v = 3b - 2018$, so $uv = 2018^2$ and $u \equiv v \equiv -2018 \equiv 1 \pmod 3$ (as $2018 = 3 \cdot 672 + 2$). Since $a \geq 1$ we have $u \geq 3 - 2018 > -2018$, and likewise $v > -2018$. If u and v were both negative,

then $|u|, |v| < 2018$ and $uv < 2018^2$, a contradiction; and $uv > 0$ rules out mixed signs. So u, v are positive divisors of 2018^2 with $u \equiv 1 \pmod 3$, and conversely each such u gives $v = 2018^2/u$, which is automatically $\equiv 1 \pmod 3$ because $uv = 2018^2 \equiv 1$; then $a = (u + 2018)/3$ and $b = (v + 2018)/3$ are positive integers.

Now $2018 = 2 \cdot 1009$, and 1009 is prime (it is not divisible by any prime up to $31 < \sqrt{1009}$: e.g. $1009 = 7{\cdot}144{+}1 = 11{\cdot}91{+}8 = 13{\cdot}77{+}8 = 17{\cdot}59{+}6 = 19{\cdot}53{+}2 = 23{\cdot}43{+}20 = 29{\cdot}34{+}23 = 31{\cdot}32{+}17$). The divisors of $2018^2 = 2^2 \cdot 1009^2$ are $2^i 1009^j$ with $0 \le i, j \le 2$, and since $2 \equiv -1$, $1009 \equiv 1 \pmod 3$, the divisor is $\equiv (-1)^i \pmod 3$. So $u \in \{1, 4, 1009, 4 \cdot 1009, 1009^2, 4 \cdot 1009^2\}$, six values, giving six ordered pairs:

$$(a, b) \in \{(673, 1358114),\ (674, 340033),\ (1009, 2018),\\ (2018, 1009),\ (340033, 674),\ (1358114, 673)\}.$$

For instance $u = 1$ gives $a = 2019/3 = 673$ and $b = (2018^2 + 2018)/3 = 2018 \cdot 673 = 1358114$; $u = 4$ gives $a = 674$ and $b = (1009^2 + 2018)/3 = 1020099/3 = 340033$; $u = 1009$ gives $a = 1009$, $b = (4 \cdot 1009 + 2018)/3 = 2018$; the remaining three are the same pairs reversed. □

Problem 4. ⋆⋆ *(Putnam 2016 A1) Find the least j such that $2016 \mid p^{(j)}(k)$ for every integer-coefficient polynomial p and every integer k.*

Key idea. The j-th derivative of x^m is $j!\binom{m}{j}x^{m-j}$, so $j!$ always divides $p^{(j)}(k)$; compare $v_p(j!)$ with $2016 = 2^5 \cdot 3^2 \cdot 7$.

Solution. The answer is $j = 8$.

$j = 8$ works. Write $p(x) = \sum_m a_m x^m$ with $a_m \in \mathbb{Z}$. Differentiating j times,

$$p^{(j)}(x) = \sum_{m \ge j} a_m\, m(m-1)\cdots(m-j+1)\, x^{m-j} = j! \sum_{m \ge j} a_m \binom{m}{j} x^{m-j},$$

and $\binom{m}{j}$ is an integer, so $p^{(j)}(k)$ is $j!$ times an integer for every $k \in \mathbb{Z}$. Since $8! = 40320 = 20 \cdot 2016$, every $p^{(8)}(k)$ is divisible by 2016.

No $j \le 7$ works. Take $p(x) = x^j$; then $p^{(j)}(k) = j!$ for every k, so we need $2016 \mid j!$. For $j \le 6$ the prime 7 does not divide $j!$. For $j = 7$, Legendre's formula gives $v_2(7!) = \lfloor 7/2 \rfloor + \lfloor 7/4 \rfloor = 3 + 1 = 4 < 5 = v_2(2016)$, so $2016 \nmid 7! = 5040$ (indeed $5040/2016 = 5/2$). Hence the smallest j is 8. □

Remark. The upper bound is a special case of Pólya's observation that the polynomials $\binom{x}{j}$ form a $\mathbb{Z}$-basis of the integer-valued polynomials. In general, the least j with $N \mid p^{(j)}(k)$ for all p, k is the least j with $N \mid j!$, which Legendre's formula computes prime by prime: here $7 \mid j!$ forces $j \ge 7$ and $2^5 \mid j!$ forces $j \ge 8$.

Problem 5. ⋆⋆⋆ *(Putnam 2018 B3) Find all $n < 10^{100}$ with $n \mid 2^n$, $n - 1 \mid 2^n - 1$, and $n - 2 \mid 2^n - 2$.*

Key idea. Each condition is a divisibility between numbers of the form $2^a - 1$, and $2^a - 1 \mid 2^b - 1$ exactly when $a \mid b$; apply this three times in a row.

Solution. *Lemma.* For positive integers a, b: $2^a - 1 \mid 2^b - 1$ if and only if $a \mid b$. *Proof.* Write $b = qa + r$ with $0 \le r < a$. Since $2^a \equiv 1 \pmod{2^a - 1}$, we have $2^b - 1 = (2^a)^q 2^r - 1 \equiv 2^r - 1 \pmod{2^a - 1}$. As $0 \le 2^r - 1 < 2^a - 1$, the number $2^b - 1$ is divisible by $2^a - 1$ exactly when $2^r - 1 = 0$, i.e. $r = 0$. (In the language of orders: $\mathrm{ord}_{2^a-1}(2) = a$.) □

Step 1: n is a power of 2. If an odd prime p divided n, then $p \mid 2^n$, which is absurd. So $n = 2^m$ with $m \ge 0$. The cases $n = 1$ and $n = 2$ fail, since then $n - 1 = 0$ or $n - 2 = 0$ would have to divide the nonzero numbers (and 0 divides only 0) $2^1 - 1 = 1$ or $2^2 - 2 = 2$. Hence $m \ge 2$ and $n \ge 4$.

Step 2: the condition $n-1 \mid 2^n-1$. This reads $2^m-1 \mid 2^n-1$, which by the Lemma holds iff $m \mid n = 2^m$, i.e. iff m is a power of 2. Write $m = 2^\ell$ with $\ell \geq 1$ (as $m \geq 2$).

Step 3: the condition $n-2 \mid 2^n-2$. Since $n-2 = 2(2^{m-1}-1)$ and $2^n-2 = 2(2^{n-1}-1)$, this is equivalent to $2^{m-1}-1 \mid 2^{n-1}-1$, i.e. (Lemma) to $m-1 \mid n-1 = 2^m-1$. With $m = 2^\ell$ this says $2^\ell - 1 \mid 2^{2^\ell}-1$, which by the Lemma once more holds iff $\ell \mid 2^\ell$, i.e. iff ℓ is a power of 2.

Step 4: the size bound. Conversely, every $n = 2^{2^\ell}$ with ℓ a power of 2 satisfies all three conditions by Steps 1–3. The constraint $n < 10^{100}$ means $2^{2^\ell} < 10^{100}$. For $\ell \geq 9$ we have $2^{2^\ell} \geq 2^{512} > 2^{400} = 16^{100} > 10^{100}$, so $\ell \leq 8$, and $\ell \in \{1, 2, 4, 8\}$. For $\ell = 8$ the bound does hold: $2^{256} = 64 \cdot (2^{10})^{25} = 64 \cdot 1024^{25} = 64 \cdot (1.024)^{25} \cdot 10^{75} < 128 \cdot 10^{75} < 10^{100}$, using $1.024^{25} < e^{25 \cdot 0.024} = e^{0.6} < 2$.

Therefore the solutions are

$$n \in \{\, 2^2,\ 2^4,\ 2^{16},\ 2^{256} \,\} = \{\, 4,\ 16,\ 65536,\ 2^{256} \,\}. \qquad \square$$

Remark. The same Euclid-style argument as in the Lemma shows $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)}-1$: reducing 2^b-1 modulo 2^a-1 leaves $2^{b \bmod a}-1$, so the Euclidean algorithm on the exponents runs in parallel with the one on the numbers. This is the identity behind most "$a^n \pm 1$" divisibility problems.

Problem 6. $\star\star\star\star$ *(Putnam 2023 B5) Determine the $n \geq 1$ such that for every m coprime to n there is a permutation π of $\{1, \ldots, n\}$ with $\pi(\pi(k)) \equiv mk \pmod{n}$ for all k.*

Key idea. The question asks when multiplication by m on $\mathbb{Z}/n$ has a square root in the symmetric group; a permutation has a square root iff each even cycle length occurs an even number of times, and the Chinese remainder theorem controls the cycle structure.

Solution. The answer is: $n = 1$ and all $n \equiv 2 \pmod 4$.

Identify $\{1, \ldots, n\}$ with $\mathbb{Z}/n$ and let $\sigma_m \colon \mathbb{Z}/n \to \mathbb{Z}/n$, $\sigma_m(k) = mk$; since $\gcd(m, n) = 1$, σ_m is a bijection. The property asks for $\pi \in S_n$ with $\pi^2 = \sigma_m$.

Lemma (square roots in S_n). A permutation σ is a square in S_n if and only if, for every even ℓ, the number of ℓ-cycles of σ is even. *Proof.* Suppose first that $\sigma = \tau^2$ for some $\tau \in S_n$, and let c be a cycle of τ of length L. If L is odd, c^2 is again an L-cycle (the powers c^{2t}, $0 \leq t < L$, of a point run through the whole cycle because $\gcd(2, L) = 1$). If $L = 2\ell$ is even, c^2 splits into two ℓ-cycles (the even-indexed and the odd-indexed points). Hence in τ^2 the cycles of even length ℓ arise only from 2ℓ-cycles of τ, and they arise two at a time: their number is even. Conversely, suppose the condition holds for σ. An odd cycle $c = (a_1\, a_2 \cdots a_L)$ equals $(c^{(L+1)/2})^2$, since $c^{L+1} = c$. Two cycles of equal length, $(a_1 \cdots a_\ell)$ and $(b_1 \cdots b_\ell)$, together equal the square of $(a_1\, b_1\, a_2\, b_2 \cdots a_\ell\, b_\ell)$. Pair up the even-length cycles of σ by length and take square roots cycle by cycle; the resulting disjoint cycles multiply to a τ with $\tau^2 = \sigma$. $\square$

$n = 1$. The only π is the identity and $\pi^2 = \sigma_m$ trivially.

$4 \mid n$ *fails.* Take $m = -1$ (coprime to every n). The fixed points of σ_{-1} are the k with $2k \equiv 0$, namely $k = 0$ and $k = n/2$; the remaining $n-2$ elements pair up into $(n-2)/2$ transpositions $\{k, -k\}$. When $4 \mid n$, $(n-2)/2$ is odd, so by the Lemma σ_{-1} has no square root.

Odd $n > 1$ fails. Choose an odd prime $p \mid n$ and write $n = p^e k$ with $p \nmid k$. By the Chinese remainder theorem $\mathbb{Z}/n \cong \mathbb{Z}/p^e \times \mathbb{Z}/k$ as rings, with σ_m acting on each factor by multiplication by m. Let g be a primitive root modulo p^e (a standard theorem: $(\mathbb{Z}/p^e)^\times$ is cyclic for odd p), and choose m with $m \equiv g \pmod{p^e}$ and $m \equiv 1 \pmod{k}$ (CRT again); then $\gcd(m, n) = 1$. Consider an element (u, v) with $u \in (\mathbb{Z}/p^e)^\times$. Since $\sigma_m^t(u, v) = (g^t u, v)$ and $g^t u \equiv u$ iff $g^t \equiv 1$, the σ_m-orbit of (u, v) has length exactly $\operatorname{ord}(g) = \varphi(p^e) = p^{e-1}(p-1)$. There are $\varphi(p^e)\, k$ such elements, so they

form exactly k cycles of length $\varphi(p^e)$. If instead $p \mid u$, then either $u = 0$, a fixed point, or $u = p^s u'$ with $1 \le s < e$ and $p \nmid u'$; in the latter case $g^t u \equiv u \pmod{p^e}$ iff $p^{e-s} \mid g^t - 1$, so the orbit length of (u, v) is the order of g modulo p^{e-s}, which divides $\varphi(p^{e-s}) < \varphi(p^e)$. These elements contribute no cycles of length $\varphi(p^e)$. Thus σ_m has exactly k cycles of the even length $\varphi(p^e)$, and k is odd because n is. By the Lemma, no square root exists.

$n \equiv 2 \pmod 4$ *works.* Write $n = 2k$ with k odd, so $\mathbb{Z}/n \cong \mathbb{Z}/2 \times \mathbb{Z}/k$. Any m coprime to n is odd, so on the first factor σ_m is the identity, and $\sigma_m(\epsilon, v) = (\epsilon, mv)$. Hence σ_m preserves the two sets $\{0\} \times \mathbb{Z}/k$ and $\{1\} \times \mathbb{Z}/k$ and acts on each of them as multiplication by m on $\mathbb{Z}/k$: the two restrictions have identical cycle types. Every cycle length therefore occurs an even number of times, and the Lemma produces π with $\pi^2 = \sigma_m$.

Combining the four cases, the property holds exactly for $n = 1$ and for $n \equiv 2 \pmod 4$. □

Remark. The single choice $m = -1$ also disposes of $n \equiv 3 \pmod 4$ (there σ_{-1} has $(n-1)/2$ transpositions, an odd number), but not of $n \equiv 1 \pmod 4$: for $n = 5$, $\sigma_{-1} = (1\,4)(2\,3)$ is a square, and one needs $m = 2$, whose permutation $(1\,2\,4\,3)$ is a single 4-cycle. The primitive-root construction is what makes the odd case uniform. Note also that the sign of σ_m is not the right invariant: every square is an even permutation, but for $n = 9$, $m = 2$ one gets $\sigma_2 = (1\,2\,4\,8\,7\,5)(3\,6)$, an even permutation that is still not a square because the 6-cycle and the 2-cycle each occur once. The obstruction is the finer cycle-count condition of the Lemma.