VCSMS PRIME

Program for Inducing Mathematical Excellence
Session 11: Number Theory
October 20, 2017

Lecture problems

1. For how many integers $4 < d < 2017$ is 441 a perfect square in base d?
2. (AI16) Let N be a natural number whose base-2016 representation is ABC. Working now in base-10, what is the remainder when $N - (A + B + C + k)$ is divided by 2015, for some $k \in \{1, 2, \ldots, 2015\}$?
3. (AHSME 1993) Given $0 \leq x_0 < 1$ define x_n for all positive integers n to be $2x_{n-1}$ if $2x_{n-1} < 1$, or $2x_{n-1} - 1$ otherwise. How many x_0 satisfy $x_0 = x_5$?
4. (AIME 1986) The sequence $1, 3, 4, 9, 10, \ldots$ consists of the positive integers which are powers of three or sums of distinct powers of three. Find its hundredth term.
5. (AIME 1985) Let $a_n = 100 + n^2$ for all positive integral n. Find the maximum GCD of a_n and a_{n+1}.
6. (HMMT 2002) Find the greatest common divisor of all numbers of the form $2002^n + 2$ for $n \in \mathbb{N}$.
7. (QI11) When $2a$ is divided by 7, the remainder is 5. When $3b$ is divided by 7, the remainder is also 5. What is the remainder when $a + b$ is divided by 7?
8. (QII2) Suppose that $159aa72$ is a multiple of 2016. What is the sum of its distinct prime divisors?
9. (Canada 2003) Find the last three digits of $2003^{2002^{2001}}$.
10. Factorize 89701, 160401 and $2^{18} + 1$.
11. (QI8) How many positive divisors of 30^9 are divisible by 400,000?
12. (AI12) Let $n = 2^{23}3^{17}$. How many factors of n^2 are less than n but do not divide n?
13. (QIII5) Let $s(n)$ be the number of terminal zeroes in the decimal representation of $n!$. How many positive integers less than 2017 cannot be expressed in the form $n + s(n)$ for some positive integer n?
14. How many ordered pairs of positive unit fractions have sum $\frac{1}{6}$?

Digits and bases

- Problem 1: All of them: $441_d = 4d^2 + 4d + 1 = (2d + 1)^2$ in base 10.
- Problem 2: $N = C + 2016B + 2016^2A$ in base 10. Then $N - (A + B + C + k) = 2015B + (2016^2 - 1)A - k$, but the first two terms are divisible by 2015, so the remainder is $2015 - k$.
- Problem 3: The doubling makes us consider binary. The sequence moves the decimal point to the right.
- Problem 4: Writing in ternary, these are the numbers that only have 0 or 1, so the terms are just binary.

Divisibility

- Note $a|b$ iff $(a, b) = a$. We have $(a, b) = (a - b, b)$. This gives the Euclidean algorithm.
- Problem 5: We have $(100+n^2, 100+(n+1)^2) = (100+n^2, 2n+1) = (200+2n^2, 2n+1) = (200-n, 2n+1) = (400 - 2n, 2n + 1) = (401, 2n + 1)$.
- Problem 6: Equivalent to GCD of 2004 and $2002^n - 2002 = 2002(2002^{n-1} - 1)$. But it is well-known that $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$.

Modulo

- The integers modulo a prime form a field. Thus we have arithmetic. For composite moduli, CRT. From most to least common, know how to solve linear systems, Fermat's Little, Euler Totient, Wilson, Lucas.
- Problem 7: $2a \equiv 5 \pmod 7$ implies $a \equiv 5 \cdot 2^{-1} \pmod 7$, but the inverse of 2 is 4 (trial-and-error, or $2x + 7y = 1$.), so $a \equiv 5 \cdot 4 \equiv 6 \pmod 7$. Similarly $b \equiv 4 \pmod 7$ and $a + b \equiv 3 \pmod 7$.
- Problem 8: $159aa72 \equiv 1590072 + 1100a \equiv 1464 + 1100a \equiv 0 \pmod{2016}$. Not hard to find a.
- Problem 9: Split into mod 8 and mod 125. Binary exponentiation for 3^{52} mod 125.

Factorization

- Usually involves clever algebraic manipulation. If you end up with a number not in an obviously factorable way, always try to rewrite as difference of two squares.
- Problem 10: The first is $300^2 - 300 + 1 = (300 + 1)^2 - 900$. The second is $20^4 + 20^2 + 1 = (20^2 + 1)^2 - 20^2$. By Sophie–Germain, the last is $(1 - 2^5 + 2^9)(1 + 2^5 + 2^9)$.

Multiplicative number theory

- A function f is multiplicative if $f(mn) = f(m)f(n)$ for all $(m, n) = 1$. Such a function is determined completely by powers of primes. Examples: $\tau(n)$, number of divisors; $\sigma(n)$, sum of divisors; $\phi(n)$, number of positive integers less than and relatively prime to n.
- Problem 11: Answer is just $\tau(30^9/400{,}000)$.
- Problem 12: Each factor of n^2 has a pair that multiplies to n^2; one is smaller and one is larger than n, so $\frac{1}{2}\left(\tau(n^2) - 1\right)$ is the number of factors less than n. These overcount the factors of n, subtract $\tau(n)$.
- "Sum of divisors that are perfect squares", "that are even", "difference of divisors with odd sum of exponents and even sum of exponents", "product of divisors" or "sums of product of non-zero digits".

Valuation

- $\nu_p(n)$ is the largest power of p that divides n. Most important is $\nu_p(n!)$, which is given by de Polignac, $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots$. This allows us, for example, to compute the valuation for binomial coefficients. This is also equivalent to $(p-1)\nu_p(n!) = n - s_p(n)$ where $s_p(n)$ is the sum of the digits of n in base p.
- Problem 13: The limiting factor of 10 is 5, so $s(n) = \nu_5 n!$. The "bumps" happen at multiples of 5. Alternatively, consider base 5 and use the second version of de Polignac's.

Diophantine equations

- The building block is $ax + by = c$ for fixed a, b, c and integers x, y. Bezout's: only need to solve the case $ax + by = (a, b)$. Then we only need to find one solution by using Euclidean algorithm or trial-and-error.
- Frobenius: if $(a, b) = 1$, for nonnegative x, y, the number of positive integers that can't be written as $ax + by$ is $\frac{1}{2}(a-1)(b-1)$. Chicken McNugget: the largest that can't is $ab - a - b$.
- Finally, factorization, often SFFT, will take care of most other cases.
- Problem 14: Equation $\frac{1}{a} + \frac{1}{b} = \frac{1}{6}$ is equiv to $6a + 6b = ab$, or $(6-a)(6-b) = 36$. Casework on factors.