Basic Training in Number Theory

Parker Glynn-Adey

January 21, 2019

1 Advice and Suggestions

- Try out lots of examples.
- The small numbers are your friends.

2 Facts and Questions

Fact 1. *If $a, b \in \mathbb{Z}$ we write $a|b$ for the statement "a divides b." Formally, $a|b$ means $b = ka$ for $k \in \mathbb{Z}$.*

Question 1. *What is the largest n such that $n^3 + 100$ is divisible by $n + 10$? Idea: Find a factorization $n^3 + 100 = (n + 10)(...) \pm C$ where C is a small constant.*

Fact 2. *The "divisors" of k are all d such that $d|k$. We say p is "prime" if its divisors are $\{1, p\}$. We say that k is "composite" if it is not prime.*

Fact 3 (Fundamental Theorem of Arithmetic)**.** *Any natural number n is a product of a unique list of primes.*

Question 2. *Show that $\sqrt{2}$ is irrational. Generalize!*

Question 3. *Show that there are infinitely many primes. Euclid's idea: Suppose there are finitely many $\{p_1, p_2, \ldots, p_n\}$ and consider $N = p_1 p_2 \ldots p_k + 1$.*

Question 4. *Show that there are arbitrarily large gaps between primes. That is, show that for any k there are k consecutive numbers $n, n + 1, \ldots, n + k$ which are all composite.*

Question 5 (Germany 1995)**.** *Consider the sequence $x_0 = 1$ and $x_{n+1} = ax_n + b$. Show that this sequence contains infinitely many composite numbers.*

3 Congruence

Fact 4 (The Division Algorithm)**.** *For any* $a, b \in \mathbb{N}$ *there is a unique pair* (k, r) *such that* $b = ka + r$ *and* $0 \leq r < a$*.*

Fact 5. *We write* $a \equiv b \mod n$ *if* $n|(a - b)$*. For any* $a \in \mathbb{Z}$ *there is* $r \in \{0, 1, \ldots, n-1\}$ *such that* $a \equiv r \mod n$*. We say that "a is congruent to r modulo n". Congruence preserves the usual rules of arithmetic regarding addition and multiplication.*

Question 6. *Suppose that* n *has digits* $n = [d_1 \ldots d_k]$ *in decimal notation.*

1. *Show that* $n \equiv d_1 + d_2 + \cdots + d_k \mod 9$*.*
2. *Show that* $n \equiv d_k \mod 10$*.*
3. *Show that* $n \equiv \sum_{k=0}^{n} (-1)^k d_k \mod 11$*.*
4. *Show that* $n \equiv [d_{k-1} d_k] \mod 100$*.*

Question 7. *What are the last two digits of* 7^{40001}*?*

Question 8. *Show that any perfect square* n^2 *is congruent to* 0 *or* $1 \mod 4$*. Conclude that no element of* $\{11, 111, 1111, \ldots\}$ *is a perfect square.*

Question 9. *Show that 3 never divides* $n^2 + 1$*.*

4 The Euclidean Algorithm

Fact 6. *The "greatest common divisor" of* a *and* b *is:*

$$\gcd(a, b) = \max\{d : d|a \text{ and } d|b\}$$

Question 10. *Show that* $\gcd(a, b) = \gcd(a, r)$ *where* $b = ak + r$ *and* (k, r) *is the unique pair of numbers given by the division algorithm.*

Question 11. *The Fibonacci numbers*[1] *are defined so that* $F(1) = 1, F(2) = 1$*, and* $F(n) = F(n-1) + F(n-2)$ *for* $n > 2$*. Show that* $\gcd(F_n, F_{n-1}) = 1$*.*

[1] The Fibonacci numbers have the following curious property: Consecutive Fibonacci numberss are the worst-case scenario for the Euclidean Algorithm. In 1888, Lamé showed: If $a \leq b \leq F_n$ then the Euclidean algorithm takes at most n steps to calculate $\gcd(a, b)$.

4.1 Parity

Question 12. *Suppose that* $n = 2k + 1$ *is odd and* $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ *is a permutation. Show that the number*

$$(1 - f(1))(2 - f(2)) \ldots (n - f(n))$$

must be even.

Question 13. *A room starts empty. Every minute, either one person enters or two people leave. Can the room contain* 2401 *people after* 3000 *minutes? Idea: Consider the "mod-3 parity" of room population.*

5 Contest Problems

Question 14. *Show that* $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ *is not an integer for any* $n > 1$.

Idea: Consider the largest power $2^k < n$. *Divide out by this largest power. This will make all of the denominators odd. (In fancy number theory terms, you're using a 2-adic valuation.)*

Question 15 (Rochester 2012)**.** *Consider the positive integers less than or equal to one trillion, i.e.* $1 \leq n \leq 10^{12}$. *Prove that less than a tenth of them can be expressed in the form* $x^3 + y^3 + z^4$ *where* x , y , *and* z *are positive integers.*

Idea: None of x, y, *or* z *can be very big. For example,* $x < \sqrt[3]{10^{12}} = 10^4$.

Question 16 (Rochester 2003)**.** *An* n*-digit number is "*k*-transposable" if* $N = [d_1 d_2 \ldots d_n]$ *and* $kN = [d_2 d_3 \ldots d_n d_1]$. *For example,* $3 \times 142857 = 428571$ *is* 3*-transposable. Show that there are two 6-digit numbers which are 3-transposable and find them.*

Big Idea: Consider repeating decimal expansions.
Observe that $10 \times 0.[d_1 d_2 d_3 \ldots] = d_1.[d_2 d_3 d_4 \ldots]$.
Find a number with a repeating decimal of length six.

Question 17. *Suppose that you write the numbers* $\{1, 2, \ldots, 100\}$ *on the blackboard. You now proceed as follows: pick two numbers* x *and* y, *erase them from the board, and replace them with* $xy + x + y$. *Continue until there is a single number left. Does this number depend on the choices you made?*