Math 43900 Problem Solving
Fall 2017
Lecture 7 Number Theory

Andrei Jorza

These problems are taken from the textbook, from Engels' *Problem solving strategies*, from Ravi Vakil's Putnam seminar notes and from Po-Shen Loh's Putnam seminar notes.

Number Theory

There are three main themes that show up in competition style number theory related problems: modular arithmetic, diophantine equations and divisibility. There's lots of other themes and ideas, such as infinite descent, integral functions and inequalities, you can see lots of these ideas in the textbook. Number theory is too vast and diverse to capture in one lecture or one collection of a dozen exercises, especially when it is combined with combinatorics. My best suggestion is to try to get a feel for what's out there from the examples and exercises in the textbook.

The main useful facts are:

1. Every integer can be written uniquely as a product of prime numbers, up to permutations of the prime factors.
2. If p is a prime number and a is not divisible by p then $a^{p-1} \equiv 1 \pmod p$. More generally, if n is an integer, $\varphi(n) = n\prod_{p|n}(1-1/p)$ where the product is over the prime divisors of n, each prime appearing a single time. Then if a is coprime to n then $a^{\varphi(n)} \equiv 1 \pmod n$.
3. If p is a prime number then the exponent of p in the prime factorization of $n!$ is $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots$.
4. (Bézout's identity) If m and n are two integers with gcd d there exist integers a and b such that $am + bn = d$. This also works for polynomials over fields, which is likewise extremely useful.

Modular arithmetic

Easier

1. This is an arch-problem, useful for the other ones.
   (a) What kinds of residues do squares have mod 3?
   (b) What kinds of residues do squares have mod 5?
   (c) What kinds of residues do squares have mod 11?
   (d) What kinds of residues do cubes have mod 9?
2. Show that the equation $x^2 + x + 1 = 11y$ has no integer solutions. [Hint: mod 11.]
3. Supose p is a prime $\equiv 3 \pmod 4$. If $p \mid x^2 + y^2$ then $p \mid x$ and $p \mid y$. [Hint: If not, then -1 would be a square mod p.]

4. Show that 2002^{2002} cannot be written as a sum of three cubes. [Hint: mod 9.]
5. Consider the sequence (a_n) defined recursively by $a_1 = 2$, $a_2 = 5$, and $a_{n+1} = (2-n^2)a_n + (2+n^2)a_{n-1}$ for $n \geq 2$. Do there exist indices p, q, r such that $a_p a_q = a_r$? [Hint: mod 3.]
6. Consider two integers $a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 3$. Show that a has a prime divisor $\equiv 3 \pmod 4$ and b has a prime divisor $\equiv 2 \pmod 3$.

Harder

7. Solve in the integers $2^x \cdot 3^y = 1 + 5^z$. [Hint: Mod 4 and mod 9.]
8. (This one is very nice and related to a problem from the handout on polynomials) Let $P(X), Q(X) \in \mathbb{Z}[X]$ be two polynomials of degrees m and n, such that every coefficient of $P(X)$ or $Q(X)$ is either 1 or 2017. If $P(X) \mid Q(X)$ show that $m + 1 \mid n + 1$. [Hint: mod 3.]
9. Use the Problems 6 and 1 to find all integers n such that $2^n - 1 \mid a^2 + 1$ for some integer a. (A harder version replaces $a^2 + 1$ with $a^2 + 9$.)

Divisibility and equations

Easier

10. Pythagorean triples. Show that the only solutions to $x^2 + y^2 = z^2$ in the integers are of the form $x = d(m^2 - n^2)$, $y = 2dmn$ and $z = d(m^2 + n^2)$ (up to signs).
11. Consider the sequence (a_n) defined by $a_0 = A \in \mathbb{Z}_{\geq 1}$ and $a_{n+1} = a_n - k^2$ where k^2 is the largest perfect square $\leq a_n$. Show that the sequence (a_n) becomes stationary if and only if A is a perfect square. [Hint: If a_n is not a perfect square then it has to be between two consecutive perfect squares. Deduce that the same is true of a_{n+1}.]
12. Find the integers n such that $\dfrac{n^3 - 3n^2 + 4}{2n - 1}$ is an integer.
13. Show that in the product $1! \cdot 2! \cdot 3! \cdots 99! \cdot 100!$ one factor can be removed to get a perfect square.
14. Is it possible to place 2015 integers on a circle such that for every pair of adjacent numbers the ratio of the larger one to the smaller one is a prime? [Hint: It's important that 2015 is odd.]
15. Show that $2^n \nmid n!$ for any $n \geq 1$.

Harder

16. As an application to Problem 1 show that the system of equations

$$\begin{cases} 5x^2 + y^2 = z^2 \\ x^2 + 5y^2 = t^2 \end{cases}$$

has no integer solutions. [Hint: Add them up.]

17. (Putnam 1999) Let $\mathcal{S}$ be a finite set of integers, each > 1. Suppose that for each integer n there is some $s \in \mathcal{S}$ such that either $(s, n) = 1$ or $(s, n) = 1$. Show that there exist $s, t \in \mathcal{S}$ such that (s, t) is a prime number. [Hint: Seek the smallest positive integer that has common factors with every element of $\mathcal{S}$.]