Stuff Mod a Prime (and Maybe Mod Other Things)

Gabriel Carroll

MOP 2010 (Black)

A good reference for a lot of the basics in this lecture is Ireland and Rosen, *A Classical Introduction to Modern Number Theory*.

I'll write $\mathbb{Z}/p\mathbb{Z}$ to denote the integers modulo a prime p. What are some things you should know about this gadget?

The most important thing you should know is that it is a *field*: you can add, subtract, multiply, and divide, and all the usual properties are satisfied. This means you can apply the binomial theorem, uniquely factor polynomials into irreducibles, and so forth.

The second most important thing you should know is Fermat's Little Theorem: $a^{p-1} = 1$ for all $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Among other things, this implies that we have the factorization

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))$$

and so any calculation you could do with roots of unity in $\mathbb{C}$ you can also do with the numbers $1, \ldots, p-1$ as $(p-1)$th roots of unity in $\mathbb{Z}/p\mathbb{Z}$. It also implies that "inversion is a polynomial," since $a^{-1} = a^{p-2}$ for $a \neq 0$, and that makes calculations easier.

The third most important thing you should know is that there always exists a *primitive root*: a number ω such that the powers of ω trace out all the different nonzero elements of $\mathbb{Z}/p\mathbb{Z}$. From this it's easy to show that the sequence $1, \omega, \omega^2, \omega^3, \ldots$ is periodic with period $p-1$. In particular, if $d \mid p-1$ then the dth powers mod p are exactly the numbers ω^{kd} for integers k, and they are exactly the numbers a such that $a^{(p-1)/d} = 1$. Also, for *any* d, the dth powers are the same as the $(gcd(d, p-1))$th powers.

We often talk about the *order* of a (nonzero) number a, as the smallest k such that $a^k = 1$. Clearly, primitive roots are exactly the numbers with order $p-1$.

What are the next most important things you should know? Here are a bunch of important facts, none of which are hard to prove if you know the above.

- Wilson's Theorem: $(p-1)! \equiv -1 \bmod p$.
- -1 is congruent to a square mod p if $p \equiv 1 \bmod 4$, and not if $p \equiv -1 \bmod 4$. (Proving full quadratic reciprocity is significantly harder.)
- For any positive integer d, $0^d + 1^d + 2^d + \cdots + (p-1)^d \equiv 0 \bmod p$ if $p-1 \nmid d$, and $\equiv -1 \bmod p$ if $p-1 \mid d$. Consequently, if P is a polynomial over $\mathbb{Z}/p\mathbb{Z}$, of degree less than $p-1$, then $P(0) + P(1) + \cdots + P(p-1) = 0$.

- Chevalley's Theorem: If $P(x_1, \ldots, x_n)$ is polynomial in n variables over $\mathbb{Z}/p\mathbb{Z}$, of degree less than n, then the number of zeroes of P is divisible by p. (In particular, if P has one known zero, it must have at least one other.)

- If x, y are elements of any extension field of $\mathbb{Z}/p\mathbb{Z}$ (for example, polynomials or power series over $\mathbb{Z}/p\mathbb{Z}$), then $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ for every positive integer n.

- Lucas's Theorem: If a, b are positive integers, with base-p representations $a_0 a_1 \ldots a_r$ and $b_0 b_1 \ldots b_r$ (with $a_i, b_i \in \{0, 1, \ldots, p-1\}$), then

$$\left(\begin{array}{c} a \\ b \end{array} \right) \equiv \left(\begin{array}{c} a_0 \\ b_0 \end{array} \right) \left(\begin{array}{c} a_1 \\ b_1 \end{array} \right) \cdots \left(\begin{array}{c} a_r \\ b_r \end{array} \right) \mod p,$$

  where we have the convention that $\left(\begin{array}{c} x \\ y \end{array} \right) = 0$ if $x < y$ and $\left(\begin{array}{c} 0 \\ 0 \end{array} \right) = 1$.

- Hensel's Lemma: If P is an integer polynomial and r an integer such that $P(r) \equiv 0 \mod p^k$, while $P'(r) \not\equiv 0 \mod p$, then r can be "lifted" to give an integer s such that $P(x) \equiv 0 \mod p^{k+1}$. Conversely, if $P(r) \equiv 0 \mod p^k$ and $P'(r) \equiv 0 \mod p$, then r cannot be lifted in this way unless $P(r) \equiv 0 \mod p^{k+1}$ already.

- Euler's extension of Fermat's theorem: If n, a are relatively prime positive integers, then $a^{\phi(n)} \equiv 1 \mod n$, where $\phi(n)$ is the Euler totient function. In particular, any integer relatively prime to n can be inverted mod n.

- If the polynomial equation $P(x_1, \ldots, x_r) = 0$ has a solution modulo m and it also has a solution modulo n, where m, n are relatively prime, then it has a solution modulo mn. (This is immediate from the Chinese Remainder Theorem. It implies that to study an equation modulo any integer n, it suffices to study it modulo the prime-power factors of n.)

- If $a \equiv b \mod n$, then $ma \equiv mb \mod mn$. (This is obvious, but often useful for calculating things modulo composite numbers. For example, if you want to calculate something mod p^2, you can look for ways to write it as $px + y$, where x can be identified mod p and y is some constant.)

Here are a bunch of problems. I've tried to arrange these into a few categories.

Calculation modulo primes and modulo powers of primes:

1. [Putnam, 1983] Let p be an odd prime. Let $F(n) = 1 + 2n + 3n^2 + \cdots + (p-1)n^{p-2}$. Prove that if a, b are integers and $F(a) \equiv F(b) \mod p$, then $a \equiv b \mod p$.

2. [USSR Book] If p is a prime greater than 3, prove that the numerator of

$$\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{p-1}$$

   is divisible by p^2.

3. [Ireland & Rosen] Calculate the sum of all the primitive roots in $\mathbb{Z}/p\mathbb{Z}$. (Your answer will depend on p.)

4. For which natural numbers n does there exist a primitive root modulo n (that is, a number whose powers modulo n represent every residue class relatively prime to n)?

5. [USSR Book] Prove that 2 is a primitive root modulo 5^n for all n.

6. [Putnam, 1991] Let p be an odd prime. Prove that

$$\sum_{j=0}^{p} \binom{p}{j} \binom{p+j}{j} \equiv 2^p + 1 \qquad \mod p^2.$$

7. Let $a_1 = 3$ and define $a_{n+1} = (3a_n^2 + 1)/2 - a_n$ for $n \geq 1$. If n is a power of 3, prove that a_n is divisible by n.

8. [AMM, 1999] Let p be a odd prime. Prove that

$$\sum_{i=1}^{p-1} 2^i \cdot i^{p-2} = \sum_{i=1}^{(p-1)/2} i^{p-2} \mod p.$$

9. [Putnam, 1996] If $p > 3$ is prime and $k = \lfloor 2p/3 \rfloor$, prove that the sum

$$\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{k}$$

is divisible by p^2.

10. [China, 2009] Given a prime number p, prove that the number of integers n such that $p|n! + 1$ is at most $cp^{2/3}$, where c is some constant independent of p.

11. [IMO Shortlist, 2008] Let n be a positive integer. Show that the numbers

$$\binom{2^n - 1}{0}, \binom{2^n - 1}{1}, \binom{2^n - 1}{2}, \ldots, \binom{2^n - 1}{2^{n-1} - 1}$$

are congruent modulo 2^n to $1, 3, 5, \ldots, 2^n - 1$ in some order.

12. [AMM, 1999] Let $p \geq 5$ be prime, and let n be an integer such that $(p+1)/2 \leq n \leq p-2$. Let $R = \sum(-1)^i \binom{n}{i}$, where the sum is taken over all $i \in \{0, 1, \ldots, n-1\}$ such that $i+1$ is a quadratic residue modulo p, and let N be the corresponding sum over nonresidues. Prove that exactly one of R and N is divisible by p.

13. [MOP, 2000] If p is a prime greater than 5, prove that $\binom{qp}{p} \equiv q \bmod p^3$, for all positive integers q.

14. [TST, 2010] Determine whether or not there exists a positive integer k such that $p = 6k + 1$ is prime and
$$\binom{3k}{k} \equiv 1 \mod p.$$

15. [IMO Shortlist, 2001] Let $p \geq 5$ be prime. Prove that there exists an integer a with $1 \leq a \leq p-2$ such that neither $a^{p-1} - 1$ nor $(a+1)^{p-1} - 1$ is divisible by p^2.

Using orders to solve Diophantine equations:

16. [IMO proposal, 1985] For $k \geq 2$, let $n_1, n_2, \ldots, n_k$ be positive integers such that
$$n_2 \mid 2^{n_1} - 1; \quad n_3 \mid 2^{n_2} - 1; \quad \ldots; \quad n_k \mid 2^{n_{k-1}} - 1; \quad n_1 \mid 2^{n_k} - 1.$$
Prove that $n_1 = n_2 = \cdots = n_k = 1$.

17. [China, 2009] Let $a > b > 1$ be integers with b odd, and n be a positive integer. Suppose $b^n \mid a^n - 1$. Prove that $a^b > 3^n/n$.

18. [IMO, 1999] Find all pairs (n, p) of positive integers such that
- p is prime;
- $n \leq 2p$;
- $(p-1)^n + 1$ is divisible by n^{p-1}.

19. [IMO, 1990] Determine all positive integers n such that $(2^n + 1)/n^2$ is an integer.

Combinatorial applications:

20. Let $k, n \in \{1, 2, \ldots, p-2\}$, where p is an odd prime. Let $S = \{1, 2, \ldots, n\} \subseteq \mathbb{Z}/p\mathbb{Z}$. If $ka \in S$ for all $a \in S$, prove that $k = 1$.

21. [Putnam, 1991] Let p be an odd prime. How many elements $x \in \mathbb{Z}/p\mathbb{Z}$ have the property that x and $x + 1$ are both squares?

22. [USSR Book] The number triangle

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & 1 & 1 & & \\ & 1 & 2 & 3 & 2 & 1 & \\ 1 & 3 & 6 & 7 & 6 & 3 & 1 \\ & & & \vdots & & & \end{array}$$

is formed by drawing two diagonals of 1's, and letting each interior number be the sum of the number just above it, the number above and to the left, and the number above and to the right. Prove that every row, starting from the third, contains at least one even number.

23. [Putnam, 2000] Let S_0 be a finite set of integers. Recursively define S_n as follows: $a \in S_{n+1}$ if and only if exactly one of $a-1, a$ is in S_n. Prove that there are infinitely many integers N such that

$$S_N = S_0 \cup \{a + N \mid a \in S_0\}.$$

24. [MOP RTC, 1999] Let p be a prime and d a factor of $p-1$. Prove that for every integer n, there exist integers $a_1, \ldots, a_d$ such that

$$a_1^d + a_2^d + \cdots + a_d^d \equiv n \mod p.$$

25. [Erdős-Ginsburg-Ziv Theorem] Given $2n-1$ integers, prove that one can choose n of them whose sum is divisible by n.