Stuff Mod a Prime (and Maybe Mod Other Things) (Teacher's Edition)

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 $p - 1 \not| \, d$, 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
$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_r}{b_r} \qquad \bmod p,$$
where we have the convention that $\binom{x}{y} = 0$ if $x < y$ and $\binom{0}{0} = 1$.

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

- Euler's extension of Fermat's theorem: If n, a are relatively prime positive integers, then $a^{\phi(n)} \equiv 1 \bmod n$, 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 $a \equiv b \bmod n$, then $ma \equiv mb \bmod mn$. (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 $F(a) \equiv F(b) \bmod p$, then $a \equiv b \bmod p$.

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.

Solution: by adding opposite terms and dividing by p, we want to show that $\sum_1^{(p-1)/2} 1/a(p-a)$ is divisible by p. Can do this by rewriting as $\sum a^{p-2}(p-a)^{p-2}$ and summing.

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

$\mu(p-1)$

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.

Solution: induction. If $2^{5^n-5^{n-1}}-1$ is divisible by 5^{n+1}, but it doesn't hold for n replaced by $n-1$, then $x^4+x^3+x^2+x+1$ is divisible by 25 where $x=2^{5^{n-1}-5^{n-2}}$. But x is a power of 16. Can check that powers of 16 are $1, 16, 6, 21, 11, 1$ mod 25, and so the $x^4+\cdots+1=0$ condition is never satisfied.

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

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

Use $\binom{p+j}{j} \equiv 1 \bmod p$ except when $j=p$.

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.

Easy to check $a_n=(2^{2^n+1}+1)/3$. So it's enough to show that $3n \mid 2^{2^n+2}-1$ when n is a power of 3 (then factor). By Euler, enough to show $2n \mid 2^n+2$, or $n \mid 2^n+1$. This holds by induction.

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

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

Solution: Expand the left side as $\sum_{j\leq i}\left(\begin{array}{c} i \\ j \end{array}\right)/i$. Summing over j, and using the fact that (for fixed j) we're summing a polynomial i over all i except p, the left side becomes $\sum_{i=1}^{p-1}(-1)^i/i$. This equals $2(\sum_{i=1}^{(p-1)/2}(-1)^i/i) = 2(1/2+1/4+\cdots+1/(p-1))$ which is the right side.

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

$$\left(\begin{array}{c} p \\ 1 \end{array}\right)+\left(\begin{array}{c} p \\ 2 \end{array}\right)+\cdots+\left(\begin{array}{c} p \\ k \end{array}\right)$$

is divisible by p^2.

Solution: Dividing through by p, quickly see that the goal is $\sum_1^k(-1)^i/i \equiv 0 \bmod p$. If $p = 6r+1$, so that $k = 4r$, then write the sum as $\sum_{i=1}^{4r} 1/i - 2\sum_1^{2r} 1/2i = \sum_{2r+1}^{4r} 1/n$ and now we can pair up opposite terms to get 0. If $p = 6r+5$ then $k = 4r+3$ and we do the same thing.

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.

clearly $n < p$; consider successive values of n satisfying the congruence, then $n!/n'! \equiv 1$ so each n is the solution to $n(n-1)\cdots(n-k+1) \equiv 1$ for some k, the "length" of n. there are at most k values of any given length k; letting x_k be the number of pairs of successive n's of distance k, we have $\sum_k x_k = r$ (the overall number of integers) and $\sum kx_k =$ total distance $\leq p$, from which it's straightforward linear maximization

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

$$\left(\begin{array}{c} 2^n-1 \\ 0 \end{array}\right),\left(\begin{array}{c} 2^n-1 \\ 1 \end{array}\right),\left(\begin{array}{c} 2^n-1 \\ 2 \end{array}\right),\ldots,\left(\begin{array}{c} 2^n-1 \\ 2^{n-1}-1 \end{array}\right)$$

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

know they're all odd; need to show they're different mod 2^n. consider ratios of successive terms — each is a number that's odd and in fact -1 mod 4. want to prove no product of consecutive ratios is 1 mod 2^n. would have to be evenly many terms. can't contain the 2^{n-2}th product since this is the only one that's not -1 mod 8. then it has to be all before or all after that product; then there's only one that's not -1 mod 16, so that value also has to be skipped, and so forth.

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 $R = \sum(-1)^i\left(\begin{array}{c} n \\ i \end{array}\right)$, 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.

Solution: $R + N = (-1)^{n-1}$ and, writing quadratic character as $(i+1)^{(p-1)/2}$, we get $R - N =$ (all but one term of an iterated difference operator on the polynomial $(x+1)^{(p-1)/2}) = \pm 1$.

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.

    Solution: Consider coefficient of x^p in $(1+x)^{qp} = (1+px+\cdots+x^p)^q$. Working mod p^3, it suffices to consider the terms of the multiplied-out thing that have at most 2 "middle" factors $\binom{p}{i} x^i$. The ones with 0 middle factors are q terms x^p; there are no terms with 1 middle factor; and the ones with 2 middle factors have a factor of p^2, and we can check that when divided by p^2 we get a thing that sums to 0 mod p.

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

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.

    for each a between 1 and $p-1$, check $a, p-a$ can't both have their $(p-1)$st powers be 1 mod p^2 (by subtracting them and binomially expanding). so at least half the numbers have $(p-1)$st powers not congruent to 1. so we win unless all odd numbers yield 1 mod p^2. check that $(p-2)^{p-1}, (p-4)^{p-1}$ can't both be 1 mod p^2 by expanding.

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 $n_1 = n_2 = \cdots = n_k = 1$.

    Solution: If one is 1 then they all are. Otherwise, consider the lowest prime dividing n_i; n_{i-1} must have a lower factor by looking at orders of 2.

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 $a^b > 3^n/n$.

    assume $b = p$ is an odd prime. $v_p(a^n - 1) = v_p(a^d - 1) + v_p(n/d)$ (where d is order of a mod p) $\leq v_p(a^d - 1) + v_p(n)$ giving $p^n \leq n(a^d - 1) < na^p$.

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}.

Solution: $n = 1$ always works. Otherwise let q be the smallest prime factor of n. Note n is odd unless $n = p = 2$ (which works). $2n$ is divisible by the order of $p-1$ mod q, so this order is 1 or 2. Either way, $q \mid p(p-2)$. If $q = p$ then $n = q = p$ and 3 is the only possible value. Otherwise $p \equiv 2$ mod q, so 2 is divisible by q, not possible.

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

    Solution: n is odd; let p be the smallest prime factor. Order of 2 mod p divides $2n$, so it's 2, and $p = 3$. Now write $n = 3^m k$, $3 \nmid k$. Now $2^n + 1 = (3-1)^n + 1$ expanded by binomial theorem is $3n+$ (terms divisible by 3^{m+2},) hence $m = 1$ since we need divisibility by n^2. Now $n = 3k$, and if $k > 1$ use the order of 8 mod the smallest prime divisor of k to get a contradiction. So only $n = 1$ works.

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 $k = 1$.

    just take sums, get $kn(n+1)/2 = n(n+1)/2$ so $k = 1$

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?

    there are $p-1$ solutions of $(a+b)(a-b) = 1$; each x with the above property corresponds to 4 such solutions, except 0 and possibly -1, so there are $(p+3)/4$ if $p \equiv 1$ mod 4 and $(p+1)/4$ if $p \equiv -1$

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

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

gen funcs mod 2

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.