

The Structure of $\mathbb{Z}/p\mathbb{Z}$

Gabriel D. Carroll, Berkeley Math Circle

April 1, 2001

The field of integers modulo a prime: one of the most elementary and elemental of number-theoretic structures. But beware; this creature is not so demure as it seems. As we begin to explore it, prepare to enter a world filled with adventure and ongoing mystery.

Okay, enough advertisement. Let's get down to business.

1 Planting the fields

We'll assume some basic knowledge. We'll assume familiarity with the various definitions of primes: $p > 1$ is prime if it cannot be factored as a product of two integers greater than 1; equivalently, whenever integers a, b satisfy $p \mid ab$, then $p \mid a$ or $p \mid b$; equivalently, whenever $p \nmid a$, the greatest common divisor of p and a (written (p, a)) is 1. We'll assume familiarity also with unique prime factorization and with basic properties of congruences.

Given a prime p , let $\mathbb{Z}/p\mathbb{Z}$, also written \mathbb{F}_p , denote the p -element set $\{0, 1, 2, \dots, p-1\}$, with operations of addition and multiplication defined modulo p .

Usually, one thinks of \mathbb{F}_p as the set of equivalence classes of integers, where two integers are equivalent if they are congruent modulo p ; here we consider it instead to be set-theoretically contained in \mathbb{Z} , because this will prove slightly more convenient later. It's evident that our arithmetic operations are well-defined on this set. We claim that \mathbb{F}_p is a *field*: that the two operations of addition and multiplication satisfy the associative, commutative, and distributive laws, that each operation has an identity (0 for addition and 1 for multiplication), that every element has an additive inverse, and that every element except 0 has a multiplicative inverse. All of the properties except for the last follow readily from the corresponding properties of addition and multiplication among the integers, so detailed proofs won't be needed. Showing the existence of multiplicative inverses is slightly harder. We give two proofs.

Suppose $a \in \mathbb{F}_p, a \neq 0$. Then $p \nmid a$, so $(a, p) = 1$. Then, the Euclidean algorithm gives integers k, l such that $ak + pl = 1$ in \mathbb{Z} ; so, $ak \equiv 1$ modulo p . Thus, reducing k modulo p gives an inverse for a in \mathbb{F}_p .

A more constructive proof follows from this

Theorem. (Fermat's Little Theorem) For a any integer, $p \mid a^p - a$.

Proof. We use induction. If $a = 0$, the statement is obvious. Now, given the statement for a , we seek to prove it for $a + 1$. But

$$(a + 1)^p - (a + 1) = \sum_{k=0}^p \binom{p}{k} a^k - a - 1.$$

For $0 < k < p$, $\binom{p}{k} = p!/k!(p-k)!$ is divisible by p , so the above sum is congruent modulo p to $(a^p + 1) - a - 1 = a^p - a \equiv 0$, giving the induction step. So now the statement holds for all $a \geq 0$. But if a is negative, there is some $a' > 0$ which is congruent to a modulo p ; since the statement holds for a' , it holds for a . ■

If $a \in \mathbb{F}_p$ is nonzero, Fermat tells us that $p \mid a(a^{p-1} - 1)$; since p is prime, $p \mid a^{p-1} - 1$, or $a^{p-1} = 1$ in \mathbb{F}_p . So, a^{p-2} is an inverse for a . We now have proved

Fact. \mathbb{F}_p is a field.

In particular, nonzero elements of \mathbb{F}_p may be meaningfully raised to any integral power, positive or negative.

It may seem confusing to let the numbers $0, 1, \dots, p-1$ denote elements both of \mathbb{F}_p and of the integers \mathbb{Z} , since the operations are defined differently, but the alternative would be notational bureaucracy, so we'll continue relying on context to make the difference clear as long as possible. When we declare explicitly that variables lie in \mathbb{F}_p , however, all operations done on them will also occur in \mathbb{F}_p unless otherwise stated.

2 May I take your order?

Whoopee, so we've got this field, and we can do calculations in it. For example, we can calculate $1 + 2 + \dots + n = n(n+1)/2$, just like in the integers. And we can add any number to itself repeatedly. In fact, if $a \in \mathbb{F}_p$ is nonzero, then the numbers $a, 2a, 3a, \dots, (p-1)a$ are just $1, 2, 3, \dots, p-1$ in some order. (Proof: We claim $0, a, 2a, \dots, (p-1)a$ are all distinct, which would prove our claim. Indeed, if integers $0 \leq i < j \leq p-1$ satisfy $ia = ja$ in \mathbb{F}_p , then $(i-j)a$ is divisible by p , but neither $i-j$ nor a is, contradiction.) It would be nice if we understood the multiplicative behavior of the elements of \mathbb{F}_p , too.

Casting aside 0 for the moment because it's boring, let a be any other element of \mathbb{F}_p . We consider the sequence a, a^2, a^3, a^4, \dots . Eventually, this sequence has a 1 in it. For example, by Fermat, $a^{p-1} = 1$. Let $o(a)$, the *order* of a (modulo p), be the smallest natural number such that $a^{o(a)} = 1$. For example, $o(1) = 1$, and $o(-1) = 2$ if $p > 2$.

Fact. Let m be an integer; then $a^m = 1$ iff $o(a) \mid m$.

Proof. We can do a division: $m = qo(a) + r$, where $0 \leq r < o(a)$. Now, $a^m = a^r$ since $a^{qo(a)} = 1^q = 1$; hence, $a^m = 1$ iff $a^r = 1$. But this happens exactly when $r = 0$, since, by definition, no positive number $r < o(a)$ satisfies $a^r = 1$. ■

It follows that the powers of a are periodic with period $o(a)$, since $a^{m+o(a)} = a^m a^{o(a)} = a^m$. Moreover, the numbers $a^1, a^2, \dots, a^{o(a)}$ are all distinct: if some two of these, say a^i, a^j for integers $i < j$, were equal, then $a^{j-i} = 1$ but $0 < j-i < o(a)$, contradiction.

Now, by combining the above proposition with Fermat, we see that every nonzero element of \mathbb{F}_p has order dividing $p-1$. We might wonder whether every order $d \mid p-1$ is achieved. In particular, we could wonder whether there is an element a whose order is precisely $p-1$ — the maximum possible order, based on what we know so far. If such an a existed, that would be awesome. Why? Because the numbers a, a^2, \dots, a^{p-1} would be distinct; since there are $p-1$ of them and they are all nonzero, they must be precisely $1, 2, \dots, p-1$ in some order. Thus, every nonzero element of \mathbb{F}_p would be a power of a . This means, for example, that multiplicative problems could be reduced to additive problems, by looking just at the exponents of a .

An element of \mathbb{F}_p with this happy property — its order is $p-1$ — is called a *primitive root*. We're going to find out when primitive roots exist — and, more generally, answer the questions raised by the above paragraph — fairly shortly. First, we need some preliminaries.

We define the *Euler totient function* $\phi(n)$ as follows: for n any positive integer, $\phi(n)$ is the number of elements of the set $\{1, 2, 3, \dots, n\}$ that are relatively prime to n . This is fairly easy to compute with. For example, if p_1, p_2, \dots, p_r are the distinct prime factors of n , then $\phi(n) = n \cdot \prod_{j=1}^r (p_j - 1)/p_j$. (Prove it!) Even without this fact, it's obvious that $\phi(n) \geq 1$, since 1 is relatively prime to n for all n .

Fact. For any positive integer n , $\sum_{d \mid n} \phi(d) = n$.

Proof. (one of many) Write the fractions $1/n, 2/n, 3/n, \dots, n/n$. Now reduce each fraction to lowest terms. The denominator of each fraction is some divisor d of n . How many fractions will have denominator d ? Well, k/n reduces to have denominator d precisely when n/d is the greatest common divisor of k and n — that is, when kd/n is an integer relatively prime to $nd/n = d$. Since k may range from 1 to n , kd/n may be any integer from 1 to d , relatively prime to d , which means that there are $\phi(d)$ such fractions. So, for each $d \mid n$, there are $\phi(d)$ fractions with denominator d , and the total number of fractions is n ; this completes the proof. ■

Now let's deal with another subject. When one is confronted with a field, there is a natural human instinct to think about *polynomials over* that field — that is, polynomials whose coefficients lie in the field. There are the usual operations on these polynomials: we can add them (by adding coefficients of like terms); we can multiply them (using the distributive law, as we do for the familiar real or complex polynomials); we can take their degrees; we can plug in values for the variable and see what comes out. Moreover, we can talk

about divisibility of polynomials and their greatest common divisor, just as we do in the real (or complex, or rational) case. For example, we have the following:

Fact. If $P(x)$ is a nonzero polynomial over any field K , and $r \in K$ satisfies $P(r) = 0$, then $P(x) = (x - r)Q(x)$ for some polynomial Q over K , where $\deg Q = \deg P - 1$.

Proof. The usual long division algorithm applies in any field: by successively eliminating terms of P , we can obtain polynomials Q, R such that $P(x) = (x - r)Q(x) + R(x)$ and R has lower degree than the divisor, $x - r$. Then, R is constant. But plugging in $x = r$ gives $0 = P(r) = (r - r)Q(r) + R(r) = R(r)$, so R is the zero polynomial, as desired. The last statement about degrees follows from the usual degree addition formula for products. ■

Now, if s is another root of P , different from r , then $0 = P(s) = (s - r)Q(s)$, so s must also be a root of Q . This easily lets us show that any (nonzero) polynomial of degree d , over any field, can have at most d roots in that field. Indeed, this holds by induction. If $d = 0$, the polynomial is a nonzero constant and so has no roots. If the statement holds for some d , and P has degree $d + 1$, then let r be a root (if P has no roots then we are done); we have $P(x) = (x - r)Q(x)$, where Q has at most d roots; taking these together with the one root r gives at most $d + 1$ roots for P , proving the assertion.

This is all we need to know about polynomials at the moment. Later on, we'll examine these creatures again.

Now, we can get back to our inquiries about orders. So, we'll return to work in the particular field \mathbb{F}_p . If $d \mid p - 1$, then the above considerations show that the polynomial $x^d - 1$ can have at most d roots in \mathbb{F}_p — that is, there are at most d elements of order dividing d .

For each $d \mid p - 1$, let $\psi(d)$ be the number of elements of \mathbb{F}_p whose order is exactly d . We claim that $\psi(d) \leq \phi(d)$ for each d . Indeed, suppose this is false, and let d be a minimal counterexample. We then have $\psi(c) = \phi(c)$ for each $c < d$, while $\psi(d) > \phi(d)$. So, the number of elements whose order divides d is

$$\sum_{c \mid d} \psi(c) > \sum_{c \mid d} \phi(c) = d,$$

contradicting the observation in the previous paragraph. This contradiction shows that our claim was true after all.

But we know that all the nonzero elements of \mathbb{F}_p have order dividing $p - 1$. So,

$$p - 1 = \sum_{d \mid p-1} \psi(d) \leq \sum_{d \mid p-1} \phi(d) = p - 1,$$

which is only possible if equality holds for each d . So, this proves the big, important

Theorem. If d is a divisor of $p - 1$, then \mathbb{F}_p has $\phi(d)$ elements of order d . In particular, there are $\phi(p - 1) \geq 1$ primitive roots.

3 Reaping what we've shown

In fact, the number of elements of each order can be obtained simply from the knowledge of the existence of a primitive root. For let a be a primitive root; we will calculate the order of a^k for any integer k . To do this, just note that $o(a^k)$ is the smallest number o such that $a^{ko} = 1$. But $a^{ko} = 1$ iff $p - 1 \mid ko$; letting $d = (p - 1, k)$, this is equivalent to $(p - 1)/d \mid ok/d$. Since $(p - 1)/d$ and k/d are relatively prime, the smallest value of o is $(p - 1)/d$. Thus, we have shown that the order of a^k is $(p - 1)/(p - 1, k)$ for each k . In particular, the various primitive roots are the numbers a^k , where k is relatively prime to $p - 1$.

Another consideration is k th powers. Since the nonzero elements of \mathbb{F}_p are $a, a^2, a^3, \dots, a^{p-1}$, the k th powers are $a^k, a^{2k}, a^{3k}, \dots, a^{(p-1)k}$. But these may not all be different. How many distinct k th powers do we have? Well, $a^{ik} = a^{jk}$ iff $p - 1 \mid (j - i)k$. Letting $d = (p - 1, k)$, this is the same as having $(p - 1)/d \mid (j - i)k/d$; equivalently (by coprimality), $(p - 1)/d \mid j - i$. Since i, j range from 1 to $p - 1$, it is evident that, for any fixed i , there are exactly d possible values of j satisfying $a^{ik} = a^{jk}$. Thus, in our list $a^k, a^{2k}, a^{3k}, \dots, a^{(p-1)k}$, each number occurs $d = (p - 1, k)$ times. Dividing out, we then see that there are exactly $(p - 1)/d$ nonzero

d th powers in \mathbb{F}_p (other than zero, which we still disdain). Moreover, each such d th power has exactly d d th roots.

Lest this get too abstract, let's take an example: $\mathbb{F}_{11} = \{0, 1, 2, 3, \dots, 10\}$. With some experimentation, we can find that 2 is a primitive root modulo 11; its successive powers are

$$2, 4, 8, 5, 10, 9, 7, 3, 6, 1.$$

The even-numbered terms are then the squares, and, as we would expect, there are five of them:

$$4 = 2^2 = 9^2; \quad 5 = 4^2 = 7^2; \quad 9 = 8^2 = 3^2; \quad 3 = 5^2 = 6^2; \quad 1 = 10^2 = 1^2.$$

What about fourth powers? We would expect there to be $10/(10, 4) = 5$ of them too, and sure enough, every square is a fourth power:

$$4 = 8^4 = 3^4; \quad 5 = 2^4 = 9^4; \quad 9 = 5^4 = 6^4; \quad 3 = 4^4 = 7^4; \quad 1 = 10^4 = 1^4.$$

And how about fifth powers? The above predicts two fifth powers, each with five fifth roots. Let's check:

$$10 = 2^5 = 8^5 = 10^5 = 7^5 = 6^5; \quad 1 = 4^5 = 5^5 = 9^5 = 3^5 = 1^5.$$

For one more example, let's consider the cubes. We expect to find $10/(10, 3) = 10$ of them. And, in accordance with prognostications,

$$2 = 7^3; \quad 4 = 5^3; \quad 8 = 2^3; \quad 5 = 3^3; \quad 10 = 10^3; \quad 9 = 4^3; \quad 7 = 6^3; \quad 3 = 9^3; \quad 6 = 8^3; \quad 1 = 1^3.$$

In group-theoretic terms (which may make all these considerations clearer), we've shown that the group of nonzero elements of \mathbb{F}_p under multiplication is isomorphic to the group of integers modulo $p - 1$ under addition. Taking k th powers in \mathbb{F}_p corresponds to multiplying by k in the additive formulation.

Let's look at some other exciting implications. For example, there's the ever-famous

Theorem. (Wilson's Theorem) If p is an odd prime, $(p - 1)! \equiv -1 \pmod{p}$.

Proof. Let a be a primitive root. Then, $1, 2, \dots, p - 1 \in \mathbb{F}_p$ are equal, in some order, to a, a^2, \dots, a^{p-1} . So, $(p - 1)!$ is congruent to $a \cdot a^2 \cdots a^{p-1} = a^{p(p-1)/2}$. Now, $a^{p(p-1)} = 1$, but $a^{p(p-1)/2} \neq 1$ since $p(p-1)/2$ is not divisible by $p - 1$ (what with p being odd). However, the equation $x^2 - 1 = 0$ can only have two solutions in \mathbb{F}_p , so these must be 1 and -1 . We conclude $a^{p(p-1)/2} = -1$, proving Wilson's theorem. ■

That was a little cheesy since Wilson's theorem can be proven in a better way. In fact, consider the polynomial $x^{p-1} - 1$. It has $p - 1$ roots in \mathbb{F}_p , namely $1, 2, \dots, p - 1$. By our earlier observations concerning the factorization of polynomials, we can completely factor $x^{p-1} - 1 = (x - 1)(x - 2)(x - 3) \cdots (x - p + 1)$. Now Wilson's theorem — along with, indeed, the values of *all* the elementary symmetric polynomials in the elements of \mathbb{F}_p — falls out by comparing coefficients. More generally, we can use this technique to compute the elementary symmetric polynomials in the d th roots of 1, for each $d \mid p - 1$.

This next result should look familiar.

Fact. Let p be an odd prime. A nonzero element $b \in \mathbb{F}_p$ is a square iff $b^{(p-1)/2} = 1$.

Proof. Let $b = a^k$ with a a primitive root. Then b is a square iff k is even (this doesn't depend on the choice of k , since the possible values of k for a given a all differ from each other by multiples of the even number $p - 1$). But k is even $\Leftrightarrow p - 1 \mid k(p - 1)/2 \Leftrightarrow a^{k(p-1)/2} = 1$. Since $a^{k(p-1)/2} = b^{(p-1)/2}$, we are done. ■

More generally, if $d \mid p - 1$, the same argument shows that b is a d th power iff $b^{(p-1)/d} = 1$.

Fact. Let p be an odd prime. Then -1 is a square modulo p iff $p \equiv 1 \pmod{4}$.

Proof. Use the above and the fact that $(-1)^{(p-1)/2} = 1$ if $p \equiv 1 \pmod{4}$, -1 if $p \equiv 3 \pmod{4}$. ■

Another application of the theory we've developed is to the solution of Diophantine equations (over the integers, not \mathbb{F}_p !). The following illustrates the general technique.

Problem. (IMO proposal, 1985) For $k \geq 2$, let n_1, n_2, \dots, n_k be positive integers such that

$$n_2 \mid 2^{n_1} - 1; \quad n_3 \mid 2^{n_2} - 1; \quad \dots; \quad n_k \mid 2^{n_{k-1}} - 1; \quad n_1 \mid 2^{n_k} - 1.$$

Prove that $n_1 = n_2 = \dots = n_k = 1$.

Solution. First note that if $n_i = 1$ for any i , then n_{i+1} (or n_1 if $i = k$) must divide $2^1 - 1 = 1$, so $n_{i+1} = 1$ also. Proceeding by induction shows that all the n_i are 1 in this case. Thus, we see that either none of the n_i are equal to 1 or all of them are. We will assume the former and obtain a contradiction.

Let p_i be the smallest prime factor of n_i , for each i . By cyclic rotation, we may assume $p_2 = \min\{p_i\}$. In particular, $p_2 \leq p_1$. Furthermore, $p_2 \neq 2$, since $p_2 \mid n_2 \mid 2^{n_1} - 1$, which is odd. Now, if o is the order of 2 modulo p_2 , we have $o \mid p_2 - 1$, so in particular $o \leq p_2 - 1$. But also $o \mid n_1$, since $p_2 \mid 2^{n_1} - 1$. However, all the prime factors of n_1 are greater than $p_1 - 1 \geq p_2 - 1$; consequently, we are forced to have $o = 1$. This means that $p_2 \mid 2^1 - 1 = 1$, an impossibility. This is the desired contradiction. ■

See the exercises for more examples of this sort.

4 Polynomials and beyond

At this point, we have understood the additive structure of \mathbb{F}_p , and we have understood the multiplicative structure of \mathbb{F}_p . However, these two operations interact in many complex and exciting ways, and many open problems exist in this area. For example: which integers are primitive roots modulo infinitely many primes? When are a number in \mathbb{F}_p and its inverse, or its square, of the same parity? When do they both lie in the set $\{1, 2, \dots, (p-1)/2\}$? To give some further idea of the richness of \mathbb{F}_p , try out some of the problems at the end of this packet.

For now, we conclude our theoretical study of the behavior of \mathbb{F}_p with a few more comments about our old friends, the polynomials over \mathbb{F}_p . As we observed earlier, a polynomial of degree d can have at most d roots. Also note the following

Fact. If m is an integer with $p-1 \nmid m$, then $1^m + 2^m + \dots + (p-1)^m = 0$ in \mathbb{F}_p .

Proof. Let a be a primitive root; then $a^m \neq 1$. Now, the numbers $a, 2a, 3a, \dots, (p-1)a$ are just $1, 2, \dots, p-1$ in some order, so

$$\begin{aligned} (1^m + 2^m + \dots + (p-1)^m)(1 - a^m) &= (1^m + 2^m + \dots + (p-1)^m) - [a^m + (2a)^m + \dots + ((p-1)a)^m] \\ &= (1^m + 2^m + \dots + (p-1)^m) - (1^m + 2^m + \dots + (p-1)^m) = 0. \end{aligned}$$

Since the second factor on the left side is nonzero, the first factor must be zero. ■

Note that, setting $0^0 = 1$, we find the preceding statement to be true for $m = 0$ also. Consequently, we have this nice

Fact. If P is a polynomial of degree less than $p-1$, then $P(0) + P(1) + \dots + P(p-1) = 0$ in \mathbb{F}_p .

Proof. Write $P(x) = \sum_{j=0}^d c_j x^j$, with $c_j \in \mathbb{F}_p$. Then

$$\sum_{i=0}^{p-1} P(i) = \sum_{i=0}^{p-1} \sum_{j=0}^d c_j i^j = \sum_{j=0}^d c_j \left(\sum_{i=0}^{p-1} i^j \right) = 0.$$

A logical extension is to consider polynomials in multiple variables. These are defined entirely analogously to real polynomials in multiple variables; a polynomial in x_1, \dots, x_n is just a formal sum of monomials of the form $c x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$, where $c \in \mathbb{F}_p$ and the e_i are nonnegative integers. The preceding proposition applies equally well to these polynomials: If *any* of the exponents e_i satisfies $e_i = 0$ or $p-1 \nmid e_i$, then

$$\sum_{x_1=0}^{p-1} \sum_{x_2=0}^{p-1} \dots \sum_{x_n=0}^{p-1} c x_1^{e_1} x_2^{e_2} \dots x_n^{e_n} = 0.$$

Indeed, the sum factors as

$$c \left(\sum_{x_1=0}^{p-1} x_1^{e_1} \right) \dots \left(\sum_{x_n=0}^{p-1} x_n^{e_n} \right),$$

and our assumption ensures that some factor is zero. This fact enables us to prove the following result about polynomials in multiple variables.

Theorem. (Chevalley’s Theorem) Let $P(x_1, \dots, x_n)$ be a polynomial over \mathbb{F}_p , of total degree less than n . Suppose P has at least one zero (that is, an n -tuple of values $(x_1, \dots, x_n), x_i \in \mathbb{F}_p$, for which P evaluates to zero). Then it has another.

Proof. In fact, we will prove the stronger assertion that the number of zeroes is divisible by p . Consider the polynomial

$$Q(x_1, \dots, x_n) = 1 - P(x_1, \dots, x_n)^{p-1}.$$

By Fermat’s Little Theorem, Q evaluates to 1 at a zero of P and 0 elsewhere. Consequently, if we can show that

$$\sum_{x_1=0}^{p-1} \sum_{x_2=0}^{p-1} \cdots \sum_{x_n=0}^{p-1} Q(x_1, \dots, x_n) = 0 \in \mathbb{F}_p, \tag{1}$$

we will be done. But the polynomial Q is a sum of monomials, one of which is the monomial 1 and the rest of which are products of $p - 1$ monomials from P . Each monomial of the latter type must have degree less than $(p - 1)n$, since each monomial of P has degree $< n$. Consequently, some variable x_i has exponent less than $p - 1$, and it follows that the sum of this monomial’s values over all n -tuples (x_1, \dots, x_n) is 0 in \mathbb{F}_p . Since this holds for each monomial in the polynomial Q , equation (1) follows, and the theorem is proven. ■

It turns out that Chevalley’s Theorem is sharp, in the sense that, for each n , there exists a degree- n polynomial in n variables with exactly one zero. However, the proof requires significantly more sophisticated machinery than we have developed here.

There is one more extremely important aspect of polynomials over \mathbb{F}_p that we have space only to touch on. That aspect is irreducibility. A nonconstant polynomial P over \mathbb{F}_p (or any fixed field) can be called *irreducible* if there do not exist nonconstant polynomials Q, R such that $P(x) = Q(x)R(x)$. One of the most natural questions to ask is: What sorts of irreducible polynomials exist? For example, over the complex numbers, the Fundamental Theorem of Algebra tells us that only degree-1 polynomials can be irreducible. And, over the reals, every irreducible polynomial has degree 1 or 2, since a real polynomial $P(x)$ has a factor of degree at most 2: let z be a complex root; if z is real then $x - z \mid P(x)$, and if z is nonreal, then \bar{z} is also a root, so $(x - z)(x - \bar{z})$ is a real polynomial dividing $P(x)$.

\mathbb{F}_p is a much smaller field, so we would expect there to be “fewer” polynomials to serve as potential factors of larger polynomials; consequently, irreducibles should abound. Sure enough, it turns out that, for every positive integer n , there exists an irreducible polynomial of degree n over \mathbb{F}_p . This fact is fundamental in the study of finite fields. Unfortunately, the proof again involves appreciably more machinery than we have been developing here.

We have been focusing on the fields \mathbb{F}_p because they are easy to understand in terms of natural numbers. However, the study of finite fields is in many ways a natural extension of the study of the prime fields \mathbb{F}_p . Many of our results — not only the existence of primitive roots, but also the results concerning d th powers, Fermat’s Little Theorem, and Chevalley’s Theorem, as well as the existence of irreducible polynomials of every degree — carry over naturally into general finite fields.

5 Acknowledgement

Much of the material in this lecture was taken from the classic work by Ireland and Rosen, *A Classical Introduction to Modern Number Theory*, published by Springer-Verlag. If you’re not sated yet, read it.

6 Problems

Some of these problems expand on ideas presented in the theory above; others are purely recreational. None are intended to be completely trivial, though they are arranged roughly in order of difficulty. Enjoy!

1. Let p be a fixed odd prime. An infinite square grid has an integer written in each square so that each number is the average of the number below it and the number to its right, and such that any two squares of the same column p squares apart contain numbers which are congruent modulo p . Show that any two squares of the same row p squares apart contain numbers congruent modulo p .

2. (Turkey, 1995) Given a positive integer n , prove that the following are equivalent:

- (a) For any positive integer a , $n \mid a^n - a$;
- (b) For any prime divisor p of n , p^2 does not divide n , and $p - 1 \mid n - 1$.

3. (Balkan Olympiad, 1999) Let $p > 2$ be a prime number such that $3 \mid p - 2$. Let

$$S = \{y^2 - x^3 - 1 \mid x, y \in \mathbb{Z}, 0 \leq x, y \leq p - 1\}.$$

Prove that at most $p - 1$ elements of S are divisible by p .

4. (Bulgaria, 1996) Find all prime numbers p, q such that $pq \mid (5^p - 2^p)(5^q - 2^q)$.

5. (Germany, 1997) Define the functions

$$f(x) = x^5 + 5x^4 + 5x^3 + 5x^2 + 1,$$

$$g(x) = x^5 + 5x^4 + 3x^3 - 5x^2 - 1.$$

Find all prime numbers p for which there exists an integer x , $0 \leq x < p$, such that both $f(x)$ and $g(x)$ are divisible by p , and for each such p , find all such x .

6. Prove that every finite field contains a subfield isomorphic to \mathbb{F}_p for some p — that is, a subfield that becomes \mathbb{F}_p upon relabeling of its elements.

7. Let p be an odd prime, and let $k, n \in \{1, 2, \dots, p - 2\}$. Consider the set $S = \{1, 2, \dots, n\} \subseteq \mathbb{F}_p$. If $ka \in S$ for all $a \in S$, prove that $k = 1$.

8. Given an odd prime p , how many of the integers $i = 0, 1, 2, \dots, p - 1$ have the property that both i and $i - 1$ are quadratic residues modulo p ?

9. (from Ireland & Rosen)

- (a) Suppose $p > 3$ is a Fermat prime, i.e. $p - 1$ is a power of 2. Show that 3 is a primitive root modulo p .
- (b) Suppose p is a prime, $p \equiv 3 \pmod{8}$, and further suppose $(p - 1)/2$ is also a prime. Show that 2 is a primitive root modulo p .

10. Prove two generalizations of Fermat's Little Theorem:

- (a) (Euler's Theorem) If a, n are two relatively prime natural numbers, $a^{\phi(n)} \equiv 1 \pmod{n}$.
- (b) In a q -element field, $x^q = x$ for all x .

11. (Turkey, 1997) Prove that, for each prime $p \geq 7$, there exists a positive integer n and integers $x_1, \dots, x_n, y_1, \dots, y_n$ not divisible by p , such that

$$x_1^2 + y_1^2 \equiv x_2^2 \pmod{p},$$

$$x_2^2 + y_2^2 \equiv x_3^2 \pmod{p},$$

\vdots

$$x_n^2 + y_n^2 \equiv x_1^2 \pmod{p}.$$

12. (Putnam, 1987) Suppose p is an odd prime. Let F be the set of ordered pairs of elements of \mathbb{F}_p , not both equal to zero, and let S be a subset of F with the property that whenever $(a, b) \in F$, exactly one of (a, b) and $(-a, -b)$ is in S . Let N be the number of elements in the intersection $S \cap \{(2a, 2b) \mid (a, b) \in S\}$. Prove that N is even.

13. (from Ireland & Rosen) Given p , compute the sum of all the primitive roots in \mathbb{F}_p . (Your answer will depend on p .)
14. (*American Mathematical Monthly*, 1999) Let p be a prime number with $p \equiv 7 \pmod{8}$, and let $L_p = \{1, 2, \dots, (p-1)/2\}$. Prove that the sum of the quadratic residues (i.e. the squares) modulo p in L_p equals the sum of the quadratic nonresidues modulo p in L_p . (The sums are taken in \mathbb{Z} , not in \mathbb{F}_p .)
15. (*American Mathematical Monthly*, 2001) Given a prime $p \equiv 7 \pmod{8}$, evaluate

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{k^2}{p} + \frac{1}{2} \right\rfloor.$$

16. Let p be an odd prime and n a positive integer. Show the existence of primitive roots modulo p^n — that is, there exists some a such that every integer not divisible by p is congruent to some power of a modulo p^n . What happens when $p = 2$?
17. (Putnam, 1996) If $p > 3$ is a prime and $k = \lfloor 2p/3 \rfloor$, prove that the sum

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

of binomial coefficients is divisible by p^2 .

18. (Poland, 1995) Let $p \geq 3$ be a given prime. Define a sequence (a_n) by $a_n = n$ for $n = 0, 1, 2, \dots, p-1$, and $a_n = a_{n-1} + a_{n-p}$ for $n \geq p$. Determine the remainder when a_{p^3} is divided by p .
19. (MOP 1999) Let p be a prime, d a positive integer, and n any integer. Prove that one can find d or fewer d th powers whose sum is congruent to $n \pmod{p}$.
20. (*American Mathematical Monthly*, 1999) Let p be an odd prime. Prove that

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

21. (Oaz Nir, MOP 2000) Prove that $\binom{ap}{p} \equiv q \pmod{p^3}$, where p is a prime greater than 5.
22. (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} .

23. (*American Mathematical Monthly*, 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 $i \in \{0, 1, \dots, n-1\}$ such that $i+1$ is a quadratic residue modulo p , and let $N = \sum (-1)^j \binom{n}{j}$, where the sum is taken over all $j \in \{0, 1, \dots, n-1\}$ such that $j+1$ is a quadratic nonresidue modulo p . Prove that exactly one of R and N is divisible by p .
24. (IMO, 1990) Determine all positive integers n such that $(2^n + 1)/n^2$ is an integer.
25. (USAMO, 1999) Let $p > 2$ be a prime, and let a, b, c, d be integers not divisible by p , such that

$$\{ra/p\} + \{rb/p\} + \{rc/p\} + \{rd/p\} = 2$$

for any integer r not divisible by p . Prove that at least two of the numbers $a+b, a+c, a+d, b+c, b+d, c+d$ are divisible by p . (Note: $\{x\} = x - \lfloor x \rfloor$ denotes the fractional part of x .)