

## Polynomial congruences modulo a prime

MATH2068 Number Theory & Cryptography  
Week 9 Lectures 1 and 2

University of Sydney  
NSW 2006  
Australia

17th September 2007



## Residue arithmetic

Let  $m \in \mathbb{Z}^+$  and define  $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$ .

That is,  $\mathbb{Z}_m$  is the set of all residues mod  $m$ .

Define *residue addition* and *residue multiplication* to be the same as ordinary addition and multiplication followed by reduction modulo  $m$ , so that the answer is always a residue.

Residue arithmetic mod 17 has  $11 + 15 = 9$  and  $7 \times 6 = 8$ .

Let  $a, b \in \mathbb{Z}_m$ . We say that  $b$  is the *inverse* of  $a$  if  $ab = 1$  using residue multiplication.

A residue  $a \in \mathbb{Z}_m$  has an inverse if and only if  $\gcd(a, m) = 1$ .

If  $m$  is prime and  $0 \neq a \in \mathbb{Z}_m$  then  $\gcd(a, m) = 1$ .

So all nonzero residues have inverses when  $m$  is prime.

## Polynomial equations over prime fields



If  $p$  is prime then  $\mathbb{Z}_p$  with residue addition and multiplication is commonly called the *finite field with  $p$  elements*.

Magma's name for it is `FiniteField(p)`.

Many theorems about  $\mathbb{R}$  also hold true for  $\mathbb{Z}_p$  when residue arithmetic replaces ordinary arithmetic. For example:

**Theorem:** Let  $f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_2x^2 + a_1x + a_0$  be a polynomial with integer coefficients and let  $p$  be a prime. The number of  $c \in \mathbb{Z}_p$  such that  $f(c) \equiv 0 \pmod{p}$  is at most  $d$ .

If we compute  $f(c)$  using residue arithmetic rather than ordinary arithmetic then  $f(c) \equiv 0 \pmod{p}$  becomes  $f(c) = 0$ .

So this is an equivalent statement: if  $a_0, a_1, \dots, a_{d-1} \in \mathbb{Z}_p$  then the equation  $x^d + a_{d-1}x^{d-1} + \dots + a_2x^2 + a_1x + a_0 = 0$  has at most  $d$  solutions in  $\mathbb{Z}_p$  (using residue arithmetic).

## A brief sketch of the proof



The proof for  $\mathbb{Z}_p$  is just the same as the proof for  $\mathbb{R}$  and goes by induction on  $d$ , the degree of  $f(x)$ .

If  $d = 1$  then  $f(x) = x + a_0$  for some integer  $a_0$ . Obviously  $x + a_0 \equiv 0 \pmod{p}$  has just one solution:  $x \equiv -a_0 \pmod{p}$ .

Now suppose that  $d > 1$  and  $x \equiv c$  is a solution of  $f(x) \equiv 0$ .

Then  $f(x) \equiv f(x) - f(c) = (x - c)g(x)$  where  $\deg g(x) = d - 1$ .

If  $f(c') \equiv 0$  then  $(c' - c)g(c') \equiv 0 \pmod{p}$ , so that either  $c' \equiv c \pmod{p}$  or  $g(c') \equiv 0 \pmod{p}$ .

The inductive hypothesis says that  $g(x) \equiv 0$  has at most  $d - 1$  solutions; so there are at most  $d$  possibilities for  $c'$ .



## Roots of unity mod $p$



**Theorem:** For each divisor  $d$  of  $p - 1$  there are exactly  $d$  residues mod  $p$  satisfying  $x^d \equiv 1 \pmod{p}$ .

**Proof:** Write  $p - 1 = de$ .

By the previous theorem there are at least  $d$  distinct nonzero residues  $b_1, b_2, \dots, b_d$  that are  $e$ -th powers.

For each  $i$  we have  $b_i \equiv a^e \pmod{p}$  for some  $a$ , and this gives  $b_i^d \equiv a^{ed} = a^{p-1} \pmod{p}$ .

But by Fermat's Little Theorem  $a^{p-1} \equiv 1$ ; so  $b_1, b_2, \dots, b_d$  are all solutions of  $x^d \equiv 1$ .

But  $x^d - 1$  can have at most  $d$  roots mod  $p$ . So the  $d$  roots  $b_1, b_2, \dots, b_d$  are the only ones.

[Note: This also shows that the number of  $e$ -th power residues is exactly  $d = (p - 1)/e$ , since if there were more than  $x^d - 1$  would have too many roots.]

## Orders of nonzero residues



Recall that if  $0 \neq a \in \mathbb{Z}_p$  then by definition  $\text{ord}_p(a)$  is the least  $k > 0$  such that  $a^k = 1$  in residue arithmetic mod  $p$ .

For example,  $\text{ord}_{13}(5) = 4$ , since  $5^1, 5^2$  and  $5^3$  are all not equal to 1 (being 5, 12 and 8 respectively), but  $5^4 = 1$ .

We know that  $a^k = 1$  in  $\mathbb{Z}_p$  if and only if  $\text{ord}_p(a)$  is a divisor of  $k$ .

By Fermat's Little Theorem, if  $0 \neq a \in \mathbb{Z}_p$  then  $a^{p-1} = 1$ , and it follows that  $\text{ord}_p(a)$  is a divisor of  $p - 1$ .

For each  $d|p - 1$  let us define  $F(d)$  to be the number of  $a \in \mathbb{Z}_p$  with  $\text{ord}_p(a) = d$ .

Then for each positive integer  $k$ , the number of  $a \in \mathbb{Z}_p$  satisfying  $a^k = 1$  is  $\sum_{d|k} F(d)$ .

## Orders of nonzero residues (continued)



But we have shown that if  $k|p - 1$  then  $a^k = 1$  has exactly  $k$  solutions in  $\mathbb{Z}_p$ .

So  $\sum_{d|k} F(d) = k$  for all divisors  $k$  of  $p - 1$ .

For example, if  $p = 13$  we get

$$F(12) + F(6) + F(4) + F(3) + F(2) + F(1) = 12$$

$$F(6) + F(3) + F(2) + F(1) = 6$$

$$F(4) + F(2) + F(1) = 4$$

$$F(3) + F(1) = 3$$

$$F(2) + F(1) = 2$$

$$F(1) = 1$$

and back substitution gives  $F(1) = 1, F(2) = 1, F(3) = 2, F(4) = 2, F(6) = 2, F(12) = 4$ .

## The general solution



We have shown that if  $F(d)$  is the number of nonzero  $a \in \mathbb{Z}_p$  with  $\text{ord}_p(a) = d$  then

$$\sum_{d|k} F(d) = k$$

for all  $k|p - 1$ .

By the Möbius Inversion Formula it follows that

$$F(k) = \sum_{d|k} \mu\left(\frac{k}{d}\right) d$$

for all  $k|p - 1$ .

But in Week 7 we proved that  $\sum_{d|k} \mu\left(\frac{k}{d}\right) d = \phi(k)$ , where  $\phi$  is Euler's phi function.

So we have proved the following theorem.

**Theorem** Let  $p$  be a prime. For each divisor  $d$  of  $p - 1$  the number of residues  $a \pmod{p}$  such that  $\text{ord}_p(a) = d$  is  $\phi(d)$ .

## Primitive roots



For us the most important conclusion to be drawn from the preceding theorem is that there are  $\phi(p - 1)$  residues  $a$  such that  $\text{ord}_p(a) = p - 1$ .

Recall that  $\text{ord}_p(a)$  has to be a divisor of  $p - 1$ .

So  $p - 1$  is the largest value that  $\text{ord}_p(a)$  can ever take.

A residue  $a$  is called a *primitive root* mod  $p$  if  $\text{ord}_p(a) = p - 1$ .

The theorem says that there are  $\phi(p - 1)$  primitive roots.

For example, there are  $\phi(12) = 4$  primitive roots modulo 13.  
(They are 2, 6, 7 and 11.)