All Prime Numbers Have Primitive Roots

Ruben Gamboa[1] Woodrow Gamboa[2]

[1] Department of Computer Science
University of Wyoming
ruben@uwyo.edu

[2] Department of Electrical Engineering
Stanford University
woodrowg@stanford.edu

ACL2 Workshop 2022
Austin, TX

Outline

- Mathematical Context
- Polynomial Congruences
- Constructing Elements of Larger Order
- Existence of Primitive Roots

Prime Numbers

- Throughout this talk, p is a prime number
- What does that mean?

Prime Numbers

- Throughout this talk, p is a prime number
- What does that mean?

$$(\forall n)(n \in \mathbb{Z} \land 2 \leq n \land n < p \rightarrow n \nmid p)$$

Prime Numbers

- Throughout this talk, p is a prime number
- What does that mean?

$$(\forall n)(n \in \mathbb{Z} \wedge 2 \leq n \wedge n < p \rightarrow n \nmid p)$$

- In ACL2?

ACL2

- Many solutions in the ACL2 community books (some even ours)

ACL2

- Many solutions in the ACL2 community books (some even ours)
- “Trend” towards Russinoff’s definition

ACL2

- Many solutions in the ACL2 community books (some even ours)
- “Trend” towards Russinoff’s definition
- Define the function `(least-divisor k n)`
- `(primep p)` $\equiv$ `(= (least-divisor 2 p) p)`

Prime Fields

- If $n \geq 2$ is an integer, the group $\mathbb{Z}/n\mathbb{Z}$ is an additive group with elements $\{0, 1, \ldots, n-1\}$ using arithmetic modulo n
- If p is a prime, $\mathbb{Z}/p\mathbb{Z}$ is actually a field with elements $\{0, 1, \ldots, p-1\}$ using arithmetic modulo p
- The multiplicative subgroup of this field is called $(\mathbb{Z}/p\mathbb{Z})^*$ and it has the elements $\{1, \ldots, p-1\}$ with operation multiplication modulo p

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

If p is a prime number, and $a \in (\mathbb{Z}/p\mathbb{Z})^*$, then $a^{p-1} \equiv 1 \pmod{p}$.

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

If p is a prime number, and a $\in (\mathbb{Z}/p\mathbb{Z})^*$, *then* $a^{p-1} \equiv 1 \pmod{p}$.

Example: $4^{7-1} \equiv 4^6 \equiv 4096 \equiv 1 \pmod{7}$ because $4095 = 7 \times 585$.

Order of an Element

Definition

If p is a prime number, and $a \in (\mathbb{Z}/p\mathbb{Z})^*$, then the order of a, written $\operatorname{ord}(a)$, is the least positive integer k such that $a^k \equiv 1 \pmod{p}$.

Order of an Element

Definition

If p is a prime number, and $a \in (\mathbb{Z}/p\mathbb{Z})^*$, then the order of a, written $\operatorname{ord}(a)$, is the least positive integer k such that $a^k \equiv 1 \pmod{p}$.

In ACL2, build a function that computes the list $[a^1, a^2, \ldots, a^k]$ until either $a^k = 1$ or $k = p - 1$.

The order of a is the length of this list. This works because of Fermat's Little Theorem, which guarantees $\operatorname{ord}(a) \leq p - 1$.

Immediately, $a^{\operatorname{ord}(a)} \equiv 1 \pmod{p}$.

Properties of Element Order

- Remember we compute the list $[a^1, a^2, \ldots, a^k]$ where the only 1 is at the end
- Computing higher powers is equivalent to appending this list repeatedly
- The only 1s appear at multiples of k

Properties of Element Order

- Remember we compute the list $[a^1, a^2, \ldots, a^k]$ where the only 1 is at the end
- Computing higher powers is equivalent to appending this list repeatedly
- The only 1s appear at multiples of k

- If $a^n \equiv 1$, then $\mathrm{ord}(a) \mid n$
- In particular, $\mathrm{ord}(a) \mid p - 1$ (Lagrange & Fermat)

Another Property of Element Order

$$\mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$$

Another Property of Element Order

$$\mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$$

This uses the fact that inverses are unique.

Another Property of Element Order

$$\mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$$

This uses the fact that inverses are unique.

```
(defthmd order-inv
  (implies (and (fep a p)
                (not (equal 0 a))
                (primep p))
           (equal (order (inv a p) p)
                  (order a p)))
  :hints ...)
```

The Defining Property of Element Order

```
(defthmd smallest-pow-eq-1-is-order
  (implies (and (fep a p)
                (not (equal 0 a))
                (primep p)
                (posp n)
                (equal (pow a n p) 1)
                (not (exists-smaller-power-eq-1 a p n)))
           (equal (order a p) n))
  :hints ...)
```

Primitive Roots

Definition

If p is a prime number, and $g \in (\mathbb{Z}/p\mathbb{Z})^*$, then g is a primitive root of p if all elements $a \in (\mathbb{Z}/p\mathbb{Z})^*$ can be written as $a = g^n$ for some n.

This means that

$$\{g^1, g^2 \ldots, g^{p-1}\} = \{1, 2, \ldots, p-1\}$$

so all the powers of g are distinct, and $\operatorname{ord}(g) = p - 1$.

Primitive Roots

Definition

If p is a prime number, and $g \in (\mathbb{Z}/p\mathbb{Z})^*$, then g is a primitive root of p if all elements $a \in (\mathbb{Z}/p\mathbb{Z})^*$ can be written as $a = g^n$ for some n.

This means that

$$\{g^1, g^2 \ldots, g^{p-1}\} = \{1, 2, \ldots, p-1\}$$

so all the powers of g are distinct, and $\text{ord}(g) = p - 1$.

Definition

If p is a prime number, and $g \in (\mathbb{Z}/p\mathbb{Z})^*$, then g is a primitive root of p if $\text{ord}(g) = p - 1$.

Outline

Detour Alert: Polynomials

Quick Detour: Consider polynomial congruences

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n \equiv 0 \pmod{p}$$

We are interested in the number of distinct roots of such polynomials.

But notice that $x^2 + 2$ has no roots among the reals

But it **does** have a root mod 11.

Roots of Products of Polynomials

Suppose x is a root of $P(x)Q(x)$, i.e., a solution of

$$P(x)Q(x) \equiv 0 \pmod{p}$$

Then either x is a root of $P(x)$ or x is a root of $Q(x)$

Roots of Products of Polynomials

Suppose x is a root of $P(x)Q(x)$, i.e., a solution of

$$P(x)Q(x) \equiv 0 \pmod{p}$$

Then either x is a root of $P(x)$ or x is a root of $Q(x)$

Moreover $\#PQ \leq \#P + \#Q$, where $\#P$ means number of distinct roots of P

Roots of Linear Polynomials

Suppose a is a root of a **non-trivial linear polynomial** $P(x) = a_0 + a_1 x$, where $a_1 \not\equiv 0 \pmod{p}$

Then $a = -a_0 a_1^{-1} \bmod p$

So the number of roots of a non-trivial linear polynomial is exactly one

Roots of Polynomials

Suppose a is a root of

$$P(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n \equiv 0 \pmod{p}$$

Roots of Polynomials

Suppose a is a root of

$$P(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n \equiv 0 \pmod{p}$$

Using polynomial division, we can write $P(x) = (x - a)Q(x)$ where

$$Q(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$$

Roots of Polynomials

Suppose a is a root of

$$P(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n \equiv 0 \pmod{p}$$

Using polynomial division, we can write $P(x) = (x - a)Q(x)$ where

$$Q(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$$

Observation: If x is a root of $P(x)$ then either $x = a$ or x is a root of $Q(x)$

Roots of Polynomials

Suppose $P(x)$ is a non-trivial polynomial of degree $n \geq 1$.

Claim: The number of distinct roots of $P(x)$ is at most n

Roots of Polynomials

Suppose $P(x)$ is a non-trivial polynomial of degree $n \geq 1$.

Claim: The number of distinct roots of $P(x)$ is at most n

If $n = 1$, then we already know $P(x)$ has exactly one root

Roots of Polynomials

Suppose $P(x)$ is a non-trivial polynomial of degree $n \geq 1$.

Claim: The number of distinct roots of $P(x)$ is at most n

If $n = 1$, then we already know $P(x)$ has exactly one root

If $n > 1$ but $P(x)$ has no roots, then the number of roots of P is at most n

Roots of Polynomials

Suppose $P(x)$ is a non-trivial polynomial of degree $n \geq 1$.

Claim: The number of distinct roots of $P(x)$ is at most n

If $n = 1$, then we already know $P(x)$ has exactly one root

If $n > 1$ but $P(x)$ has no roots, then the number of roots of P is at most n

If $n > 1$ and a is a root of $P(x)$, then $P(x) = (x - a)Q(x)$ and

$$\#P(x) \leq \#(x - a) + \#Q(x) \leq 1 + n - 1 = n$$

Fermat's Little Theorem (Again)

Consider the polynomial congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

By Fermat's Little Theorem, this polynomial has precisely $p - 1$ roots!

The Punch Line

Now suppose $d \mid p-1$ and consider

$$x^d - 1 \equiv 0 \pmod{p}$$

The Punch Line

Now suppose $d \mid p-1$ and consider

$$x^d - 1 \equiv 0 \pmod{p}$$

We have that $cd = p-1$ for some choice of c, and we can show that

$$x^{p-1} - 1 = x^{cd} - 1 = (x^d - 1)(1 + x^d + x^{2d} + \cdots + x^{(c-1)d})$$

The polynomial on the left has precisely $p-1$ roots

The Punch Line

Now suppose $d \mid p-1$ and consider

$$x^d - 1 \equiv 0 \pmod{p}$$

We have that $cd = p-1$ for some choice of c, and we can show that

$$x^{p-1} - 1 = x^{cd} - 1 = (x^d - 1)(1 + x^d + x^{2d} + \cdots + x^{(c-1)d})$$

The polynomial on the left has precisely $p-1$ roots

The polynomial product on the right has at most $d + (c-1)d$ distinct roots

$$d + (c-1)d = d + cd - d = cd = p-1$$

The Punch Line

Now suppose $d \mid p-1$ and consider

$$x^d - 1 \equiv 0 \pmod{p}$$

We have that $cd = p-1$ for some choice of c, and we can show that

$$x^{p-1} - 1 = x^{cd} - 1 = (x^d - 1)(1 + x^d + x^{2d} + \cdots + x^{(c-1)d})$$

The polynomial on the left has precisely $p-1$ roots

The polynomial product on the right has at most $d + (c-1)d$ distinct roots

$$d + (c-1)d = d + cd - d = cd = p - 1$$

So both polynomials in the product have to have their maximum number of roots

In particular, $x^d - 1$ has **exactly** d roots

The Punch Line Translated to ACL2

```
(defthm num-roots-fermat-poly-divisor-implicit
  (implies (and (posp d)
                (primep p)
                (divides d (1- p)))
           (equal (pfield-polynomial-num-roots (fermat-poly d) p)
                  d))
  :hints ...)
```

Outline

- Mathematical Context
- Polynomial Congruences
- Constructing Elements of Larger Order
- Existence of Primitive Roots

The Strategy

We want to find an x such that $\text{ord}(x) = p - 1$

The strategy is to start with elements of smaller order, and combine them to create an element of larger order

If we keep doing this, we'll end up with the desired element of order $p - 1$ (the highest possible)

Products

Suppose $\mathrm{ord}(a) = m$ and $\mathrm{ord}(b) = n$

What can we say about $\mathrm{ord}(ab)$?

Products

Suppose $\text{ord}(a) = m$ and $\text{ord}(b) = n$

What can we say about $\text{ord}(ab)$?

In some cases, the order is mn

But in others it's 1, e.g., if $b = a^{-1}$

Products

Suppose $\text{ord}(a) = m$ and $\text{ord}(b) = n$

What can we say about $\text{ord}(ab)$?

In some cases, the order is mn

But in others it's 1, e.g., if $b = a^{-1}$

It works right when $\gcd(m, n) = 1$

Products when Orders Are Relatively Prime (1)

Suppose $\text{ord}(a) = m$, $\text{ord}(b) = n$, and $\gcd(m, n) = 1$

Products when Orders Are Relatively Prime (1)

Suppose $\text{ord}(a) = m$, $\text{ord}(b) = n$, and $\gcd(m, n) = 1$

The Easy Direction:

$$(ab)^{mn} \equiv a^{mn} b^{mn} \equiv 1 \pmod{p}$$

So $\text{ord}(ab) \mid mn = \text{ord}(a)\,\text{ord}(b)$

Products when Orders Are Relatively Prime (2)

Suppose $\operatorname{ord}(a) = m$, $\operatorname{ord}(b) = n$, and $\gcd(m, n) = 1$

Products when Orders Are Relatively Prime (2)

Suppose $\text{ord}(a) = m$, $\text{ord}(b) = n$, and $\gcd(m, n) = 1$

The Hard Direction:

Suppose $(ab)^k \equiv 1 \pmod{p}$

Then $a^k b^k \equiv 1 \pmod{p}$, so $a^k = (b^{-1})^k$

And that means $a^{nk} = (b^{-1})^{nk} = 1$

So $\text{ord}(a^k) \mid n$

Products when Orders Are Relatively Prime (2)

Suppose $\text{ord}(a) = m$, $\text{ord}(b) = n$, and $\gcd(m, n) = 1$

The Hard Direction:

Suppose $(ab)^k \equiv 1 \pmod{p}$

Then $a^k b^k \equiv 1 \pmod{p}$, so $a^k = (b^{-1})^k$

And that means $a^{nk} = (b^{-1})^{nk} = 1$

So $\text{ord}(a^k) \mid n$

And trivially $\text{ord}(a^k) \mid m$

Products when Orders Are Relatively Prime (2)

Suppose $\text{ord}(a) = m$, $\text{ord}(b) = n$, and $\gcd(m, n) = 1$

The Hard Direction:

Suppose $(ab)^k \equiv 1 \pmod{p}$

Then $a^k b^k \equiv 1 \pmod{p}$, so $a^k = (b^{-1})^k$
And that means $a^{nk} = (b^{-1})^{nk} = 1$
So $\text{ord}(a^k) \mid n$

And trivially $\text{ord}(a^k) \mid m$

Since $\gcd(m, n)$, this means $\text{ord}(a^k) = 1$, and that means $a^k = b^k = 1$

Products when Orders Are Relatively Prime (3)

Suppose $\text{ord}(a) = m$, $\text{ord}(b) = n$, and $\gcd(m, n) = 1$

Products when Orders Are Relatively Prime (3)

Suppose $\mathrm{ord}(a) = m$, $\mathrm{ord}(b) = n$, and $\gcd(m, n) = 1$

From the assumption that $(ab)^k = 1$, we now know that $a^k = b^k = 1$

Which means that $m \mid k$ and $n \mid k$

Products when Orders Are Relatively Prime (3)

Suppose $\text{ord}(a) = m$, $\text{ord}(b) = n$, and $\gcd(m, n) = 1$

From the assumption that $(ab)^k = 1$, we now know that $a^k = b^k = 1$

Which means that $m \mid k$ and $n \mid k$

Since $\gcd(m, n)$, this means $mn \mid k$

Products when Orders Are Relatively Prime (3)

Suppose $\operatorname{ord}(a) = m$, $\operatorname{ord}(b) = n$, and $\gcd(m, n) = 1$

From the assumption that $(ab)^k = 1$, we now know that $a^k = b^k = 1$

Which means that $m \mid k$ and $n \mid k$

Since $\gcd(m, n)$, this means $mn \mid k$

The only constraint on k was that $(ab)^k = 1$, so letting $k = \operatorname{ord}(ab)$ we see that

$$\operatorname{ord}(a)\operatorname{ord}(b) = mn \mid k = \operatorname{ord}(ab)$$

Products when Orders Are Relatively Prime (3)

Suppose $\operatorname{ord}(a) = m$, $\operatorname{ord}(b) = n$, and $\gcd(m, n) = 1$

From the assumption that $(ab)^k = 1$, we now know that $a^k = b^k = 1$

Which means that $m \mid k$ and $n \mid k$

Since $\gcd(m, n)$, this means $mn \mid k$

The only constraint on k was that $(ab)^k = 1$, so letting $k = \operatorname{ord}(ab)$ we see that

$$\operatorname{ord}(a)\operatorname{ord}(b) = mn \mid k = \operatorname{ord}(ab)$$

Combining the two parts

$$\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$$

Products when Orders Are Relatively Prime

```
(defthm construct-product-order
  (implies (and (primep p)
                (fep a p)
                (not (equal 0 a))
                (fep b p)
                (not (equal 0 b))
                (relatively-primep (order a p) (order b p)))
           (equal (order (mul a b p) p)
                  (* (order a p)
                     (order b p))))
  :hints ...)
```

Element of Prime Power Order (1)

Now for any prime q, we find an element with order q^k whenever $q^k \mid p - 1$

(Note that if $q^k \nmid p - 1$, then there cannot be any element of order q^k)

Element of Prime Power Order (1)

Now for any prime q, we find an element with order q^k whenever $q^k \mid p - 1$

(Note that if $q^k \nmid p - 1$, then there cannot be any element of order q^k)

Suppose that x is such that $x^{q^k} \equiv 1 \pmod{p}$

Element of Prime Power Order (1)

Now for any prime q, we find an element with order q^k whenever $q^k \mid p-1$

(Note that if $q^k \nmid p-1$, then there cannot be any element of order q^k)

Suppose that x is such that $x^{q^k} \equiv 1 \pmod{p}$

Then $\operatorname{ord}(x) \mid q^k$, which means that $\operatorname{ord}(x)$ is one of

$$1, q, q^2, \ldots, q^k$$

We show that in ACL2 by explicitly finding the exponent, which is
`(number-of-powers (order x p) q)`

Element of Prime Power Order (2)

We are looking for an element with order q^k, where $q^k \mid p - 1$

If $x^{q^k} \equiv 1 \pmod{p}$, then $\operatorname{ord}(x)$ is one of $1, q, q^2, \ldots, q^k$

Element of Prime Power Order (2)

We are looking for an element with order q^k, where $q^k \mid p - 1$

If $x^{q^k} \equiv 1 \pmod{p}$, then $\operatorname{ord}(x)$ is one of $1, q, q^2, \ldots, q^k$

Suppose $\operatorname{ord}(x) = q^i$, with $i < k$. Then for any $j > i$,

$$
\begin{aligned}
x^{q^j} &\equiv x^{q^{i+j-i}} \\
&\equiv x^{q^i q^{j-i}} \\
&\equiv \left(x^{q^i}\right)^{q^{j-i}} \\
&\equiv 1^{q^{j-i}} \\
&\equiv 1 \pmod{p}
\end{aligned}
$$

Element of Prime Power Order (2)

We are looking for an element with order q^k, where $q^k \mid p - 1$

If $x^{q^k} \equiv 1 \pmod{p}$, then $\mathrm{ord}(x)$ is one of $1, q, q^2, \ldots, q^k$

Suppose $\mathrm{ord}(x) = q^i$, with $i < k$. Then for any $j > i$,

$$\begin{aligned} x^{q^j} &\equiv x^{q^{i+j-i}} \\ &\equiv x^{q^i q^{j-i}} \\ &\equiv \left(x^{q^i}\right)^{q^{j-i}} \\ &\equiv 1^{q^{j-i}} \\ &\equiv 1 \pmod{p} \end{aligned}$$

In particular, if $\mathrm{ord}(x) = q^i$, with $i < k$ then $x^{q^{k-1}} \equiv 1 \pmod{p}$

Element of Prime Power Order (3)

We are looking for an element with order q^k, where $q^k \mid p-1$

We now that if we find an x such that

$$x^{q^k} \equiv 1 \pmod{p}$$
$$x^{q^{k-1}} \not\equiv 1 \pmod{p}$$

Then in fact $\mathrm{ord}(x) = q^k$

Element of Prime Power Order (3)

We are looking for an element with order q^k, where $q^k \mid p - 1$

We now that if we find an x such that

$$x^{q^k} \equiv 1 \pmod{p}$$
$$x^{q^{k-1}} \not\equiv 1 \pmod{p}$$

Then in fact $\mathrm{ord}(x) = q^k$

This is where we use The Punch Line!
Since there are q^k roots of $x^{q^k} - 1$, there are q^k possible xs that work for the first
(Note that we are surreptitiously using the fact that $q^k \mid p - 1$)

Element of Prime Power Order (3)

We are looking for an element with order q^k, where $q^k \mid p-1$

We now that if we find an x such that

$$x^{q^k} \equiv 1 \pmod{p}$$
$$x^{q^{k-1}} \not\equiv 1 \pmod{p}$$

Then in fact $\mathrm{ord}(x) = q^k$

This is where we use The Punch Line!
Since there are q^k roots of $x^{q^k} - 1$, there are q^k possible xs that work for the first
(Note that we are surreptitiously using the fact that $q^k \mid p-1$)

Similarly, there are q^{k-1} that falsify the second equality
So there are $q^k - q^{k-1}$ that work for both!

Element of Prime Power Order

```
(defthm order-is-prime-power
  (implies (and (primep p)
                (primep q)
                (natp n)
                (divides (expt q n) (1- p)))
           (and (fep (witness-with-order-q^n q n p) p)
                (not (= 0 (witness-with-order-q^n q n p)))
                (equal (order (witness-with-order-q^n q n p) p)
                       (expt q n))))
  :hints ...)
```

Outline

- Mathematical Context
- Polynomial Congruences
- Constructing Elements of Larger Order
- Existence of Primitive Roots

Existence of Primitive Roots (1)

Start with a prime p

Then consider $p - 1$ and factor that into prime powers

$$p - 1 = {p_1}^{k_1} \times {p_2}^{k_2} \times \cdots \times {p_m}^{k_m}$$

For each ${p_i}^{k_i}$ there is a c_i such that $\mathrm{ord}(c_i) = {p_i}^{k_i}$

Let $c = c_1 \times c_2 \times \cdots \times c_m$
Then $\mathrm{ord}(c) = {p_1}^{k_1} \times {p_2}^{k_2} \times \cdots \times {p_m}^{k_m} = p - 1$

So c is a primitive root of p

Existence of Primitive Roots (2)

```
(defun primitive-root-aux (k p)
  (if (or (zp k) (= 1 k))
      1
    (let* ((q (least-divisor 2 k))
           (n (number-of-powers k q))
           (k1 (/ k (expt q n))))
      (mul (witness-with-order-q^n q n p)
           (primitive-root-aux k1 p)
          p))))
```

Proving that this function terminates on all inputs is non-trivial

Existence of Primitive Roots (3)

```
(defthm primes-have-primitive-roots-aux
  (implies (and (primep p)
                (natp k)
                (divides k (1- p)))
           (equal (order (primitive-root-aux k p) p)
                  k))
  :hints ...)
```

This uses an induction scheme suggested by `primitive-root-aux`

Existence of Primitive Roots (4)

Many technical lemmas are required, including

- the arithmetic functions return elements in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$,
- in particular the result of those operations is never 0,
- the number kq^{-n} divides $p-1$ whenever k divides $p-1$,
- and the gcd of q^n and k/q^{-n} is 1.

Existence of Primitive Roots (5)

```
(defund primitive-root (p)
  (primitive-root-aux (1- p) p))

(defthm primes-have-primitive-roots
  (implies (primep p)
           (equal (order (primitive-root p) p)
                  (1- p)))
  :hints ...)
```

This is just a simple corollary of the previous theorem, and is a good example of the paradox of induction:

- It's often easier to prove a more general theorem.

Conclusion (and a Cry for Help)

- ACL2 can be very effective reasoning about number theory and group theory
- The proof above used many basic facts of both
- It would have been much easier if those basic facts were already known to ACL2
- It's time to build some foundational libraries of these, making it easier to reason about cryptography (say)