Lecture 5 Prime Numbers, Finite Fields, Powers, Primitive Roots

Def. An integer $p > 1$ is called **prime** if *p* has no factors other than 1 and *p* itself.

Ex.
(1) 2,3,5,7,11,13, … etc are prime numbers

(2) There are no efficient algorithms for determining whether or not a number is prime. In Sage one can use the command: in Primes(), to determine if a number is prime or the command: next_prime() to compute the next prime larger than a certain value. For example,

13567291 in Primes() = True
13567293 in Primes() = False

next_prime(13567293) = 13567297

Prop. If *p* is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$

Pf: Let $g = \gcd(a, p)$ then since $g \mid p$ we must have $g = 1$ or $g = p$.
If $g = p$ then $p \mid a$. So assume instead that $g = 1$.

By the Extended Euclidean Algorithm there exist integers *u*,*v* such that

$$au + pv = 1$$

$$abu + pbv = b$$

$$p \mid ab \text{ and } p \mid p \Rightarrow p \mid (abu + pbv) \Rightarrow p \mid b$$

Hence we have that $p \mid a$ or $p \mid b$.

The following theorem is crucial to what follows, but we will not prove the result.

Fundamental Theorem of Arithmetic
Every integer can be factored into powers of primes. The factorization is unique except for the order of the factors.

Finite Fields
Note, when *p* is a prime then every element of $(Z / pZ)^* = Z_p^* = F_p^*$ is a unit. Hence $Z / pZ = Z_p = F_p$ is a field (note in Sage we use the notation GF(p) for this field).

Powers in finite fields

Consider the following example of powers in F_7^*, note all of the calculations are done mod 7.

$\mathbf{1^1 \equiv 1, 1^2 \equiv 1, 1^3 \equiv 1, 1^4 \equiv 1, 1^5 \equiv 1, 1^6 \equiv 1}$

$\mathbf{2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1}$

$\mathbf{3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1}$

$\mathbf{4^1 \equiv 4, 4^2 \equiv 2, 4^3 \equiv 1, 4^4 \equiv 4, 4^5 \equiv 2, 4^6 \equiv 1}$

$\mathbf{5^1 \equiv 5, 5^2 \equiv 4, 5^3 \equiv 6, 5^4 \equiv 2, 5^5 \equiv 3, 5^6 \equiv 1}$

$\mathbf{6^1 \equiv 6, 6^2 \equiv 1, 6^3 \equiv 6, 6^4 \equiv 1, 6^5 \equiv 6, 6^6 \equiv 1,}$

Here are a couple of observations about this example:
(1) The powers of 3 and 5 generate all the elements of F_7^*

(2) All 6th powers are congruent to 1.

The last observation generalizes to the following theorem.

Fermat's Little Theorem
Let *p* be a prime number and let *a* be an integer. Then

$$a^{p-1} \equiv \begin{cases} 1 & \text{if } p \nmid a \\ 0 & \text{if } p \mid a \end{cases} \pmod{n}$$

Pf:
Either $p \mid a$ or $p \nmid a$
Case 1: $p \mid a$ then *p* divides all powers of *a* hence $p \mid a^{p-1} \Rightarrow a^{p-1} \equiv 0 \pmod{p}$

Case 2: $p \nmid a$. Consider the *p* – 1 numbers: $a, 2a, 3a, \ldots, (p-1)a$ reduced mod *p*. hence each of these numbers falls between1 and *p*-1.

Claim: these numbers are all distinct. Suppose not. Then $ja \equiv ka \pmod{p}$ where $1 \le j \le p-1,\ 1 \le k \le p-1$. Also assume that $j \ge k$.

$ja \equiv ka \pmod{p} \Rightarrow p \mid (j-k)a \Rightarrow p \mid (j-k)$ or $p \mid a$. But we assumed $p \nmid a$, so $p \mid (j-k)$. But we have $0 \le j-k \le p-2$. Hence it is impossible for *p* to divide $j-k$ unless $j=k$. The claim is shown.

That means that the list $a, 2a, 3a, \ldots, (p-1)a$ must contain all of the numbers 1,2…, *p*-1 in some order. We then have

$$\begin{aligned} a * 2a * \cdots * (p-1)a &\equiv 1 * 2 * \cdots * (p-1) \pmod{p} \\ a^{p-1} * (p-1)! &\equiv (p-1)! \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

In the earlier example of powers in $\boldsymbol{F}_7^*$ we observed that all 6th powers are congruent to 1. This follows from Fermat's Little Theorem since 7 – 1 = 6.

Fermat's Little Theorem gives an alternative method to compute multiplicative inverses.

For example, in Lecture 4 we computed $\mathbf{15^{-1} \bmod 23}$.

By Fermat's Little Theorem, we have $\mathbf{15^{22} \equiv 1 \pmod{23} \Rightarrow 15^{21} \equiv 15^{-1} \pmod{23}}$. Use the Fast Power Algorithm to compute $\mathbf{15^{21} \bmod 23}$.

$\mathbf{21 = 16 + 4 + 1}$

$\mathbf{15^1 \equiv 15 \pmod{23}}$

$\mathbf{15^2 \equiv 225 \equiv 18 \pmod{23}}$

$\mathbf{15^4 \equiv 18^2 \equiv 324 \equiv 2 \pmod{23}}$

$\mathbf{15^8 \equiv 2^2 \equiv 4 \pmod{23}}$

$\mathbf{15^{16} \equiv 4^2 \equiv 16 \pmod{23}}$

$\mathbf{15^{-1} \equiv 15^{21} \equiv 16 * 2 * 15 \equiv 20 \pmod{23}}$

This is the answer we previously got.

Def. Let x be any element of $\boldsymbol{F}_p^*$. The smallest positive power of x such that $\boldsymbol{x^n \equiv 1 \pmod{p}}$ is called the **order** of x.

Ex:

(1) In the powers of $\boldsymbol{F}_7^*$ example we computed earlier, we can find the orders of elements by inspection.

order(2) = 3, order(3) = 6, order(4) = 3, order(5) = 6, order(6) =2

(2) In $\boldsymbol{F}_{1009}^*$ we can use the Sage commands:

```
F = GF(1009)
order(674) = F(674).multiplicative_order() = 504
order(667) = F(667).multiplicative_order() = 1008
```

Prop. Let p be a prime and let a be any integer not divisible by p. Suppose that $\boldsymbol{a^n \equiv 1 \pmod{p}}$. Then order($p$) divides n. In particular order(p) divides p – 1

Pf. Let k = order(a), then $a^k \equiv 1 \pmod{p}$. We want to show that $k \mid n$. Divide n by k to obtain $n = kq + r \quad \text{with} \ 0 \le r < k$.

We then have $1 \equiv a^n \equiv a^{kq+r} \equiv (a^k)^q a^r \equiv 1^q a^r \equiv a^r \pmod{p}$. But $r < k$ which contradicts that k is the smallest positive power of a congruent to 1. The only possibility is that $r = 0$, which implies that k divides n. By Fermat's Little Theorem we have $a^{p-1} \equiv 1 (\text{mod } p)$ which implies that k divides $p - 1$

Def. Let p be a prime. A number $g \in F_p^*$ is called a **primitive root** if the powers of g generate all of F_p^*. Namely, $F_p^* = \{1, g, g^2, ..., g^{p-2}\}$. A primitive root has order p – 1.

Primitive Root Theorem: Let p be a prime. F_p^* has at least one primitive root.

Ex:
(1) In F_7^* we have two primate roots, 3 and 5. This is because order(3) = order(5) = 6

(2) Finding primitive roots in Sage. To find all primitive roots in F_p^*.

```
F = GF(p)
[i for i in range(1,p) if F(i).is_primitive_root()]
```

For example, for F_{1009}^* the above code produces a list of 288 primitive roots.

There is an algorithm for computing primitive roots (not efficient for large primes).

Let p be a prime. We want to find primitive roots of F_p^*. The following algorithm will find all primitive roots. If only one is needed then we can stop after the first one found.

```
Primitive Root Algorithm
Step 1: Factor $p$ – 1. Let $p_1 p_2, ..., p_r$ be the prime factors of $p$ – 1.
Step 2: For $a$ = 2 to $p$ – 1.
          Step 3: For $i$ = 1 to $r$
                    Step 4: If $a^{(p-1)/p_i} \equiv 1 \pmod{p}$
                    Step 5: Then $a$ is **not** a primitive root
          Step 6: $a$ is a primitive root
```

Ex: *p* = 761, use the above algorithm to find the first primitive root of $\boldsymbol{F}_{761}^{*}$.

$\boldsymbol{p-1=760=2^3*5*19}$. We need to check the prime factors 2, 5, 19. In order to be a primitive root a number must pass the test for each prime factor.

$\boldsymbol{a=2}$

$\mathbf{2^{380}\equiv 1\ (\text{mod}\,761)}$ **2 not a primitive root**

$\boldsymbol{a=3}$

$\mathbf{3^{380}\equiv 760\ (\text{mod}\,761)}$ **OK**

$\mathbf{3^{152}\equiv 1(\text{mod}\,761)}$ **3 not a primitive root**

$\boldsymbol{a=4}$

$\mathbf{4^{380}\equiv 1\ (\text{mod}\,761)}$ **4 not a primitive root**

$\boldsymbol{a=5}$

$\mathbf{5^{380}\equiv 1\ (\text{mod}\,761)}$ **5 not a primitive root**

$\boldsymbol{a=6}$

$\mathbf{6^{380}\equiv 760\ (\text{mod}\,761)}$ **OK**

$\mathbf{6^{152}\equiv 67\ (\text{mod}\,761)}$ **OK**

$\mathbf{6^{40}\equiv 498\ (\text{mod}\,761)}$ **OK**

Conclusion: 6 is a primitive root mod 761.

Note: If *n* is not prime we can still try to find primitive roots in $\boldsymbol{Z}_{n}^{*}$. Unfortunately the above algorithm does not work in this case. Also, there is no guarantee that $\boldsymbol{Z}_{n}^{*}$ has any primitive roots.

How do we find primitive roots in this case? Sage commands:

```
R=Integers(n)
L = R.list_of_elements_of_multiplicative_group()
print L
[i for i in L if R(i).is_primitive_root()]
```

Ex:

(1) $\boldsymbol{Z_6^{*}=\{1,5\}}$ and 5 is a primitive root

(2) $\boldsymbol{Z_{14}^{*}=\{1,3,5,9,11,13\}}$.
Primitive roots are {3, 5}

(3) $\boldsymbol{Z_{15}^{*}=\{1,2,4,7,8,11,13,14\}}$
But there are no primitive roots.

Theorem: $\boldsymbol{Z_n^{*}}$ has primitive roots if and only if $\boldsymbol{n=2,4,p^k,\text{ or }2p^k}$. In the above *n* = 6 or *n* = 14 satisfies this criteria, but 15 does not.