CS 5602 Introduction to Cryptography
Lecture 10
Chinese Remainder Theorem
Finite Fields

George Markowsky
Computer Science Department
Missouri University of Science & Technology

1

Moving 2/26 Class

- I need to be at a University of Missouri System event on Tuesday 2/26
- Consequently, I will not be here to give the lecture
- Instead I will give that lecture online, Friday 2/22 from 7:30 – 8:45 pm
- The lecture will be recorded and you will be able to access the recording in case you can't connect Friday evening
- More details later this week

2

Details for Connection

Dial-in number (US): (712) 775-7031
Access code: 479-616-524#
International dial-in numbers: https://fccdl.in/i/479-616-524
Online meeting ID: 479-616-524
Join the online meeting: https://join.freeconferencecall.com/479-616-524

Slides will be available on Canvas before the lecture in case you prefer to download them and join the meeting by phone. You can ask questions either online or by phone.

3

4

Studying $\mathbb{Z}_n$

- You have already gotten the notion that integers modulo n will be very important in cryptography
- We will now begin a deeper look at $\mathbb{Z}_n$ and its very interesting properties
- We know that $\mathbb{Z}_n$ is an additive abelian group, but $\mathbb{Z}_n - \{0\}$ is only a multiplicative group if n is a prime
- We know that the elements $q \in \mathbb{Z}_n - \{0\}$ that are relatively prime to n form an abelian, multiplicative group and that this is the largest subset of $\mathbb{Z}_n - \{0\}$ that is a multiplicative subgroup
- If p and q are integers such that GCD(p,q) = 1 we say that p and q are coprime or relatively prime

5

Equations mod n

- Suppose we have equations of the form a*x = b (mod n)
- Here are some questions
- Can we always find at least one solution for the above equation?
- Can there be more than one solution for such an equation?
- If there can be more than one solution, how many solutions can there be?
- Try some equations
- 7x = 3 (mod 143)
- 2x = 3 (mod 8)
- 11x = 22 (mod 143)

6

Equations

- 7x = 3 (mod 143) has the unique solution x = 123
- Where did that come from?
- 2x = 3 (mod 8) has no solution because 2x is always even and can never have a remainder of 3 mod 8
- 11x = 22 (mod 143) has the following 11 solutions: 2, 15, 28, 41, 54, 67, 80, 93, 106, 119, and 132 (do you see a pattern?)
- Let's approach this systematically

7

Solving ax = b (mod n)

- Note that if ax = b (mod n) this means that ∃ c such that ax + cn = b
- Note that if g = GCD(a,n), then (ax + cn) % g = 0
- In particular, there is no solution if b%g ≠ 0
- Recall the equations
- 7x = 3 (mod 143), GCD(7,143) = 1 and 3%1 = 0
- 2x = 3 (mod 8), GCD(2,8) = 2 and 3%2 ≠ 0
- 11x = 22 (mod 143), GCD(11,143) = 11 and 22%11 = 0
- Is b%g = 0 sufficient for there to be a solution of ax = b (mod n)?

8

Solving ax = b (mod n)

- Suppose b%g = 0, then b = k*g
- Note that from the extended GCD algorithm, ∃ s and t such that g = s*a +t*n, which means that k*s*a + k*t*n = k*g (mod n) which means that k*s*a = b (mod n)
- Applying this to the equation 7X = 3 (mod 143) we see that GCD(7,143) = 1, 7*41 – 2*143 = 287 – 286 = 1
- Thus, the solution is 3*41 = 123 and indeed 123*7 = 3 + 6*143
- Similarly, for 11x = 22 (mod 143) we see that 1*11 +0*143 = 11, and since 22/11 = 2, we see that x = 2 is a solution of this equation

9

Invertible Elements in $\mathbb{Z}_n$

- We have mentioned before that $\mathbb{Z}_n$ – {0} is a multiplicative group if n is a prime, but is not a group otherwise because it has zero-divisors
- We have also mentioned that $\mathbb{Z}_n^* = \{ q \in \mathbb{Z}_n \mid GCD(q,n) = 1\}$ is an abelian, multiplicative group
- Let's summarize why this is a group

1. Clearly, $1 \in \mathbb{Z}_n^*$ is a multiplicative identity
2. If, $u, v \in \mathbb{Z}_n^*$ ∃ a, b, c, d such that a*n + b*u = 1 and c*n + d*v = 1
   a. If you multiply these two equations you see that (a*c*n + a*d*v + b*c* u)n + (b*d)*uv = 1, so $uv \in \mathbb{Z}_n^*$
3. If a*n + b*v = 1, then b is the multiplicative inverse of $v \in \mathbb{Z}_n^*$

10

Multiple Solutions of ax = b (mod n)

- Suppose ax = b (mod n) and ay = b (mod n), where x and y are < n
- Then a(x-y) = 0 mod n
- So a(x-y) = kn for some k
- We know that g = GCD(a,n) so a = pg and n =qg where GCD(p,q) = 1
- Write pg(x-y) = kqg so p(x-y) = kq, since p and q are coprime, (x-y) = dq and k = dp
- Thus we see that x = y + dq for some d
- If GCD(a,n) = 1, n = q and (x-y) = 0 (mod n), i.e, the solution is unique

11

Multiple Solutions of ax = b (mod n)

- If GCD(a,n) = g and q = n/g, then given a solution y we can see that y + q will be another solution because (a*(y+q))%n = (a*y + a*q)%n = a*y%n = b
- You can also see that if y is a solution of the equation and y + d is also a solution of the equation, that a*d = 0 (mod n) which means that d is a multiple of n/g
- You can generate all solutions by starting at any solution and adding q = n/g repeatedly
- For 11x = 22, we could start with the solution 2 and repeatedly add 143/11 = 13 to get other solutions

12

Multiple Solutions of ax = b (mod n)

- You can start at any solution and derive all the other solutions by adding n/g repeatedly
- You don't have to start with the smallest root since the repeated additions will just wrap around
- Note that the solutions form a subset of $\mathbb{Z}_n$ that is closed under addition and subtraction, but it need not be a subgroup, since 0 might not be in it
- Note that the set of numbers {0, q, 2q, ..., (g-1)*q } form a subgroup
- In particular, the solutions of the equation g*x = 0 (mod n) form a cyclic subgroup of $\mathbb{Z}_n$

13

Systems of Linear Equations

- Consider the system of linear equations

1. $x = b_1 \pmod{n_1}$
2. $x = b_2 \pmod{n_2}$
3. $x = b_3 \pmod{n_3}$
4. ...
5. $x = b_k \pmod{n_k}$

- Note that the coefficients are all 1 so we know each equation has a unique solution (GCD(1,k) = 1 ∀ k)
- When can we find a solution to the entire system of equations
- This leads us to the Chinese Remainder Theorem

14

The Chinese Remainder Theorem – Wikipedia (edited)

- *The Chinese remainder theorem is a theorem of number theory, which states that if one knows the remainders of the division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime.*
- *The earliest known statement of the theorem is by the Chinese mathematician Sunzi in the 3rd century AD (not quite 2000 years).*
- *The Chinese remainder theorem is widely used for computing with large integers, as it allows replacing a computation for which one knows a bound on the size of the result by several similar computations on small integers.*
- *The Chinese remainder theorem (expressed in terms of congruences) is true over every principal ideal domain. It has been generalized to any commutative ring, with a formulation involving ideals.*

15

The Chinese Remainder Theorem

- The original statement was (Wikipedia)
- *There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there? (Sunzi, 3rd Century AD)*
- x = 2 (mod 3), x = 3 (mod 5), and x = 2 (mod 7)
- x = 128
- The first complete solution was published by a Chinese mathematician in 1247

16

The Chinese Remainder Theorem (CRT)

- Theorem (CRT): Let s and t be coprimes, then the map $f : \mathbb{Z}_{s*t} \rightarrow \mathbb{Z}_s \times \mathbb{Z}_t$ given by f(m) = (m%s, m%t) is a bijection.
- Proof: We first prove that f is an injection. Suppose f(m) = f(n) for two distinct integers.
- This means that m%s = n%s and m%t = n%t
- This means that (m-n) = 0 (mod s) and (m-n) = 0 (mod t)
- This means that (m-n) is divisible by s and by t
- Since s and t are coprime, (m-n) is divisible by s*t, so m = n (mod s*t)
- Thus, f is an injection
- Note that $|\mathbb{Z}_{s*t}| = s*t = |\mathbb{Z}_s| * |\mathbb{Z}_t| = |\mathbb{Z}_s \times \mathbb{Z}_t|$ so f must be a bijection.

17

Remarks on the CRT

- Note that the proof we gave was non-constructive in the sense that we know there is a unique solution for each set of equations, but we do not know how to find the solution for each set of equations
- We know that if GCD(s,t) = 1, then ∃ a, b such that a*s + b*t = 1
- Note that 1 = 1%s = (a*s+b*t)%s = (b*t)%s and 1 = (a*s)%t
- Suppose we want to solve x%s = m and x%t = n
- Consider the value x = n*a*s + m*b*t
- x%s = (n*a*s+m*b*t)%s = (m*b*t)%s = (m%s)*((b*t)%s) = m%s = m
- Similarly, x%t = n%t = n

18

Remarks on the CRT

- First, exactly the same proof (with induction) works on any number of factors $s_1, s_2, ..., s_k$ as long as GCD(s_i,s_j) = 1 ∀ i, j, i.e., we have that
- $\mathbb{Z}_{s_1 * s_2 \ldots s_k} \cong \mathbb{Z}_{s_1} \times \mathbb{Z}_{s_2} \cdots \times \mathbb{Z}_{s_k}$
- The symbol ≅ means isomorphism
- Note that this result is generally not true if GCD(s,t) ≠ 1
- For example, let s = 4 and t = 6 then (1%4,1%6) = (13%4,13%6) and in general (x%4,x%6) = ((x+12)%4,(x+12)%6)
- Since LCM(s,t)%s = 0 = LCM(s,t)%t, ((x+LCM(s,t))%s,(x+LCM(s,t))%t) = (x%s,x%t) we want LCM(s,t) = s*t which happens iff s and t are coprime
- Note LCM(s,t) = s*t/GCD(s,t), so we need GCD(s,t) = 1 to have a bijection

19

The Euler ϕ Function

- Let n be a positive integer > 1
- Define RP(n) = { 1 ≤ p < n | GCD(p,n) = 1 }
- RP stands for relatively prime also called coprime
- Define ϕ(n) = |RP(n)|
- Note some fonts don't have ϕ but instead have φ
- We shall accept both versions!
- Theorem 1: If p is a prime, ϕ(p) = p-1
- Proof: All the integers 1, 2, ..., p – 1 are relatively prime to p so φ(p) = p-1

20

The Euler ϕ Function

- Theorem 2: If p is a prime, $\phi(p^n) = p^{n-1}(p-1)$
- Proof: Suppose $1 < k \le p^n$ such that GCD(k,p^n) ≠ 1, then k = m*p for some m.
- The choices for m are 1, 2, ..., p^{n-1} so there are p^{n-1} numbers between 1 and p^n that are NOT relatively prime to p^n
- This means that the number of integers relatively prime to p^n is $p^n - p^{n-1} = p^{n-1}(p-1)$

21

The Euler ϕ Function

The number of integers in $\mathbb{Z}/N\mathbb{Z}$ which are relatively prime to N is given by the Euler ϕ function, $\phi(N)$. Given the prime factorization of N it is easy to compute the value of $\phi(N)$. If N has the prime factorization

$$N = \prod_{i=1}^{n} p_i^{e_i}$$

then

$$\phi(N) = \prod_{i=1}^{n} p_i^{e_i - 1}(p_i - 1).$$

Note, the last statement it is very important for cryptography: *Given the factorization of N it is easy to compute the value of $\phi(N)$.* The most important cases for the value of $\phi(N)$ in cryptography are:

(1) If p is prime then

$$\phi(p) = p - 1.$$

(2) If p and q are both prime and $p \neq q$ then

$$\phi(p \cdot q) = (p-1)(q-1).$$

I want to do this proof more carefully and generally and will do so a week from today

22

Discrete Logarithms

- From the text:
- *If g is a generator of the cyclic group G we often write G = <g>.*
- *If G is multiplicative then every element h of G can be written as $h = g^x$*
- *If G is additive then every element h of G can be written as h = x · g*
- *x in both cases is some integer called the discrete logarithm of h to the base g.*

23

Lagrange's Theorem

THEOREM 1.4 (Lagrange's Theorem). *If $(G, \cdot)$ is a group of order (size) $n = \#G$ then for all $a \in G$ we have $a^n = 1$.*

So if $x \in (\mathbb{Z}/N\mathbb{Z})^*$ then

$$x^{\phi(N)} = 1 \pmod{N}$$

since $\#(\mathbb{Z}/N\mathbb{Z})^* = \phi(N)$. This leads us to Fermat's Little Theorem, not to be confused with Fermat's Last Theorem which is something entirely different.

THEOREM 1.5 (Fermat's Little Theorem). *Suppose p is a prime and $a \in \mathbb{Z}$ then*

$$a^p = a \pmod{p}.$$

Fermat's Little Theorem is a special case of Lagrange's Theorem and will form the basis of one of the primality tests considered in a later chapter.

24

2. Finite Fields

The integers modulo a prime p are not the only types of finite field. In this section we shall introduce another type of finite field which is particularly important. At first reading you may wish to skip this section. We shall only be using these general forms of finite fields when discussing the Rijndael block cipher, stream ciphers based on linear feedback shift registers and when we look at elliptic curve based systems.

For this section we let p denote a prime number. Consider the set of polynomials in X whose coefficients are reduced modulo p. We denote this set $\mathbb{F}_p[X]$, which forms a ring with the natural definition of addition and multiplication.

Of particular interest is the case when $p = 2$, from which we draw all our examples in this section. For example, in $\mathbb{F}_2[X]$ we have

$$(1 + X + X^2) + (X + X^3) = 1 + X^2 + X^3,$$
$$(1 + X + X^2) \cdot (X + X^3) = X + X^2 + X^4 + X^5.$$

25

Just as with the integers modulo a number N, where the integers modulo N formed a ring, we can take a polynomial $f(X)$ and then the polynomials modulo $f(X)$ also form a ring. We denote this ring by

$$\mathbb{F}_p[X]/f(X)\mathbb{F}_p[X]$$

or more simply

$$\mathbb{F}_p[X]/(f(X)).$$

But to ease notation we will often write $\mathbb{F}_p[X]/f(X)$ for this latter ring. When $f(X) = X^4 + 1$ and $p = 2$ we have, for example,

$$(1 + X + X^2) \cdot (X + X^3) \pmod{X^4 + 1} = 1 + X^2$$

since

$$X + X^2 + X^4 + X^5 = (X + 1) \cdot (X^4 + 1) + (1 + X^2).$$

When checking the above equation you should remember we are working modulo two.

26

Recall, when we looked at the integers modulo N we looked at the equation

$$ax = b \pmod{N}.$$

We can consider a similar question for polynomials. Given a, b and f, all of which are polynomials in $\mathbb{F}_p[X]$, does there exist a solution α to the equation

$$a\alpha = b \pmod{f}?$$

With integers the answer depended on the greatest common divisor of a and f, and we counted three possible cases. A similar three cases can occur for polynomials, with the most important one being when a and f are coprime and so have greatest common divisor equal to one.

A polynomial is called irreducible if it has no proper factors other than itself and the constant polynomials. Hence, irreducibility of polynomials is the same as primality of numbers. Just as with the integers modulo N, when N was prime we obtained a finite field, so when $f(X)$ is irreducible the ring $\mathbb{F}_p[X]/f(X)$ also forms a finite field.

27

Consider the case $p = 2$ and the two different irreducible polynomials

$$f_1 = X^7 + X + 1$$

and

$$f_2 = X^7 + X^3 + 1.$$

Now, consider the two finite fields

$$F_1 = \mathbb{F}_2[X]/f_1(X) \text{ and } F_2 = \mathbb{F}_2[X]/f_2(X).$$

These both consist of the 2^7 binary polynomials of degree less than seven. Addition in these two fields is identical in that one just adds the coefficients of the polynomials modulo two. The only difference is in how multiplication is performed

$$(X^3 + 1) \cdot (X^4 + 1) \pmod{f_1(X)} = X^4 + X^3 + X,$$
$$(X^3 + 1) \cdot (X^4 + 1) \pmod{f_2(X)} = X^4.$$

A natural question arises as to whether these fields are 'really' different, or whether they just "look" different. In mathematical terms the question is whether the two fields are *isomorphic*. It turns out that they are isomorphic if there is a map

$$\phi : F_1 \longrightarrow F_2,$$

28