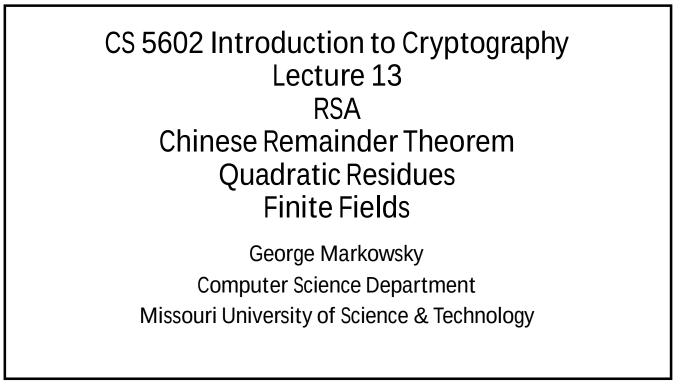
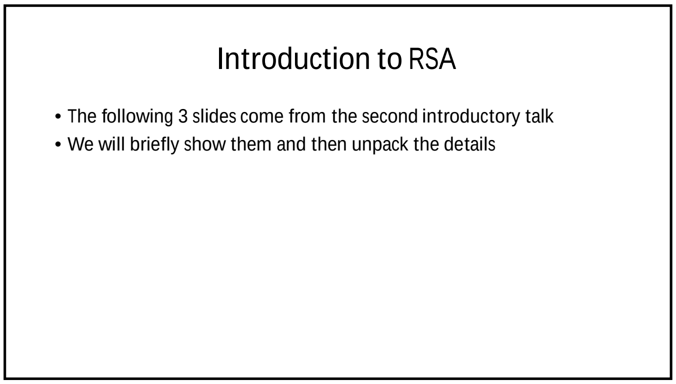


CS 5602 Introduction to Cryptography
Lecture 13
RSA
Chinese Remainder Theorem
Quadratic Residues
Finite Fields

George Markowsky
Computer Science Department
Missouri University of Science & Technology

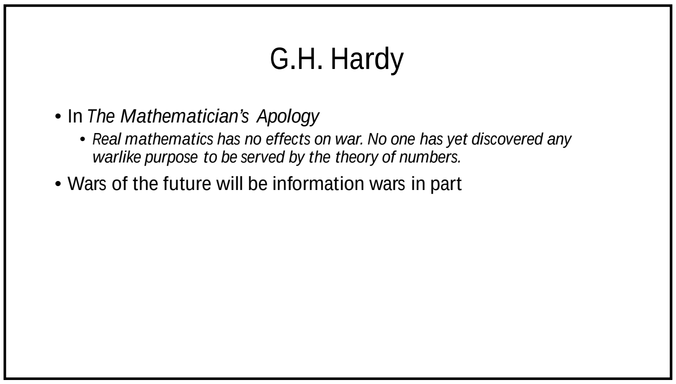
1



Introduction to RSA

- The following 3 slides come from the second introductory talk
- We will briefly show them and then unpack the details

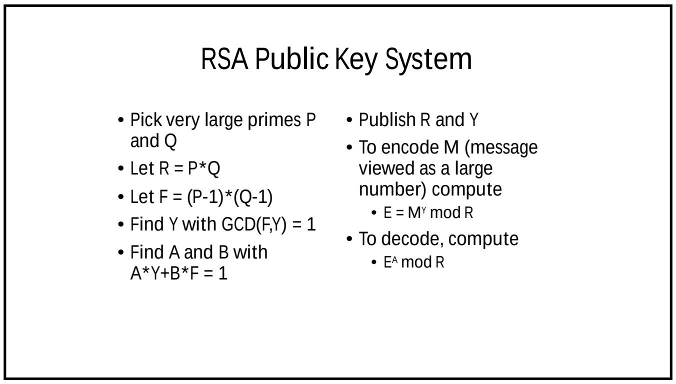
2



G.H. Hardy

- In *The Mathematician's Apology*
  - *Real mathematics has no effects on war. No one has yet discovered any warlike purpose to be served by the theory of numbers.*
- Wars of the future will be information wars in part

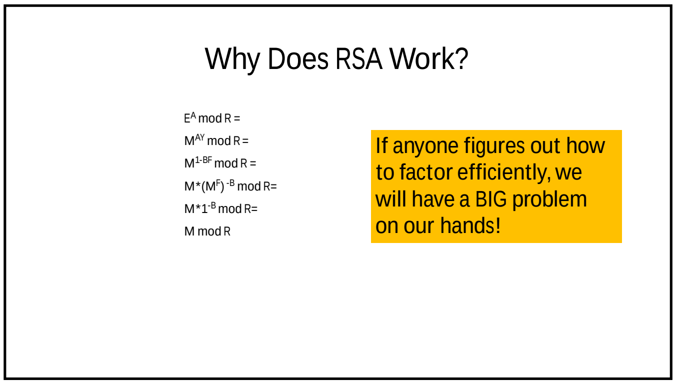
3



RSA Public Key System

- Pick very large primes P and Q
- Let R = P*Q
- Let F = (P-1)*(Q-1)
- Find Y with GCD(F,Y) = 1
- Find A and B with A*Y+B*F = 1
- Publish R and Y
- To encode M (message viewed as a large number) compute
  - $E = M^Y \bmod R$
- To decode, compute
  - $E^A \bmod R$

4



Why Does RSA Work?

E^A mod R =

M^{AY} mod R =

M^{1-BF} mod R =

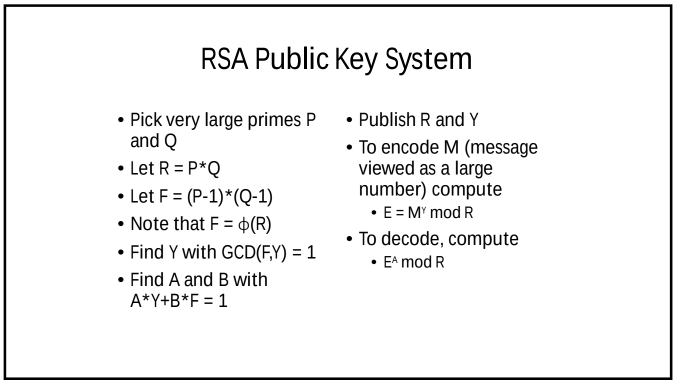
$M*(M^F)^{-B}$ mod R=

$M*1^{-B}$ mod R=

M mod R

If anyone figures out how to factor efficiently, we will have a BIG problem on our hands!

5



RSA Public Key System

- Pick very large primes P and Q
- Let R = P*Q
- Let F = (P-1)*(Q-1)
- Note that F = ϕ(R)
- Find Y with GCD(F,Y) = 1
- Find A and B with A*Y+B*F = 1
- Publish R and Y
- To encode M (message viewed as a large number) compute
  - $E = M^Y \bmod R$
- To decode, compute
  - $E^A \bmod R$

6

RSA Encryption

- r = pq (p and q are large primes)
- We will look at ($\mathbb{Z}_r$,×), let's call it $\mathbb{Z}_r$*
- Since r is not prime we are looking at the multiplicative group of units
- |$\mathbb{Z}_r$*| = φ(r) = (p-1)(q-1) = f (in the original scheme)
- Pick y coprime with f and find a and b such that
- ay + bf = 1
- Let m be our message encoded (not encrypted) as a number
- Let the encrypted message e be computed as m^a (mod r)
- That's the encryption!

7

RSA Decryption

- d = e^a (mod r)
- That's the decryption!
- Why does this work?
- e^a (mod r) = m^{ay} (mod r)
- If m ϵ $\mathbb{Z}_r$* we know that $m^{φ(r)}$ = 1 (mod r)
- In particular, m^f = $m^{φ(r)}$ = 1 (mod r), so
- m^{ay} = m^{1-bf} = mm^{-bf} = $m(m^{-b})^f$ = m (mod r) since k^f = 1 for all k ϵ $\mathbb{Z}_r$*
- That's it folks! An idea worth 100's of millions of $
- There is a slight glitch in the above presentation – can you see it?
- What if m ∉ $\mathbb{Z}_r$*?

8

m ∉ $\mathbb{Z}_r$*?

- Will cover in detail when we get to RSA in the book, but for now consider
- What are the odds that m ∉ $\mathbb{Z}_r$*?
- $\frac{(P-1)(Q-1)}{P\times Q} = 1 - \frac{P+Q}{P\times Q} + \frac{1}{P\times Q}$ = T
- What might that be?
- Let's assume that p and q are roughly the same size k, then we get 1- T = 2/k - 1/k^2 which for k > 10^{100} is < 2/10^{100} which is not very likely!

9

The Chinese Remainder Theorem (CRT)

- Theorem (CRT): Let s and t be coprimes, then the map f : $\mathbb{Z}_{s*t}$ → $\mathbb{Z}_s$ × $\mathbb{Z}_t$ 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 = |$\mathbb{Z}_s$| * |$\mathbb{Z}_t$| = |$\mathbb{Z}_s$ × $\mathbb{Z}_t$| so f must be a bijection.

10

Remarks on the CRT

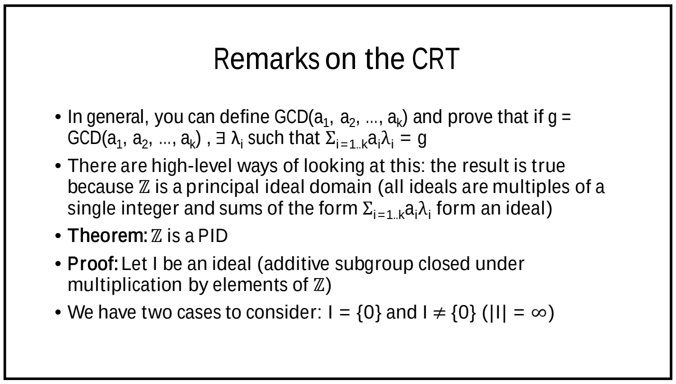
- Note that the proof we gave was non-constructive in the sense that we know there is a unique solution for each set of equations, but we do not know how to find the solution for each set of equations
- We know that if GCD(s,t) = 1, then ∃ a, b such that a*s + b*t = 1
- Note that 1 = 1%s = (a*s+b*t)%s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

11

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

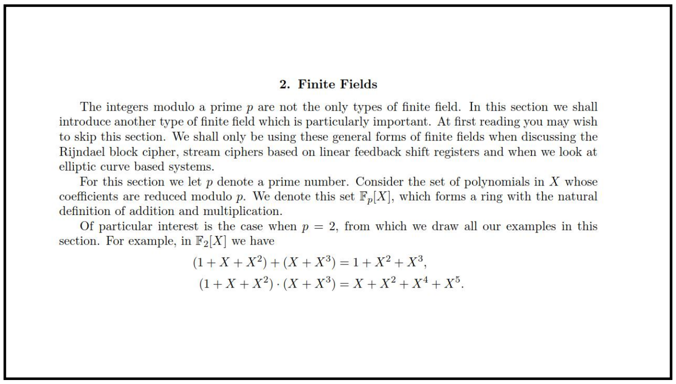
12



Remarks on the CRT

- In general, you can define GCD(a_1, a_2, …, a_k) and prove that if g = GCD(a_1, a_2, …, a_k) , ∃ λ_i such that $\Sigma_{i=1..k} a_i \lambda_i$ = g
- There are high-level ways of looking at this: the result is true because ℤ is a principal ideal domain (all ideals are multiples of a single integer and sums of the form $\Sigma_{i=1..k} a_i \lambda_i$ form an ideal)
- **Theorem:** ℤ is a PID
- **Proof:** Let I be an ideal (additive subgroup closed under multiplication by elements of ℤ)
- We have two cases to consider: I = {0} and I ≠ {0} (|I| = ∞)

13



2. Finite Fields

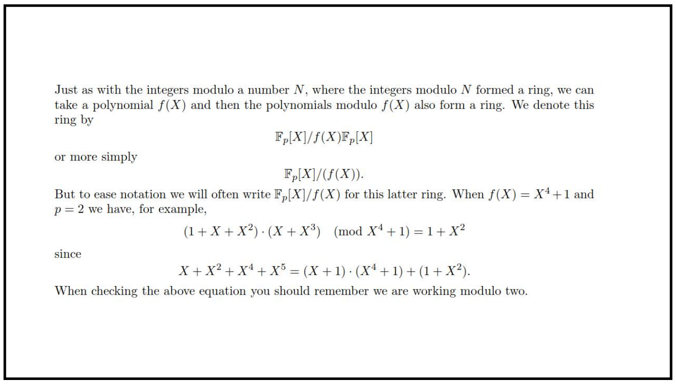
The integers modulo a prime p are not the only types of finite field. In this section we shall introduce another type of finite field which is particularly important. At first reading you may wish to skip this section. We shall only be using these general forms of finite fields when discussing the Rijndael 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

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

14



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,

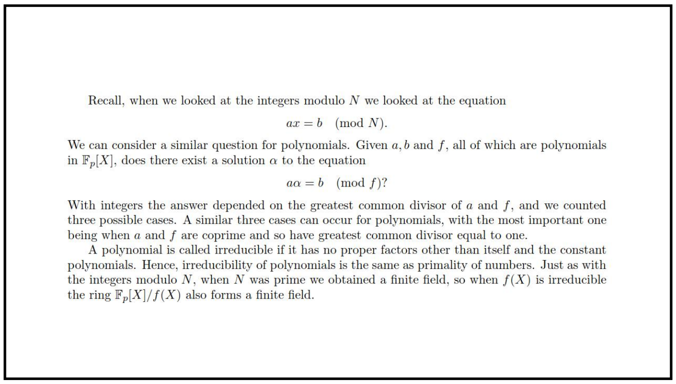
$$(1 + X + X^2) \cdot (X + X^3) \pmod{X^4 + 1} = 1 + X^2$$

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.

15



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

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

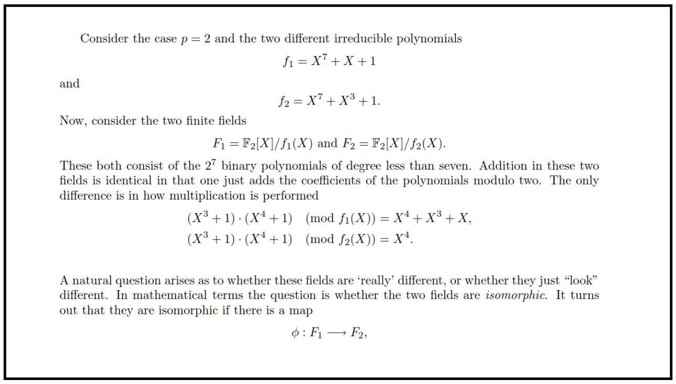
We can consider a similar question for polynomials. Given a, b and f, all of which are polynomials in $\mathbb{F}_p[X]$, does there exist a solution α to the equation

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

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.

16



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

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

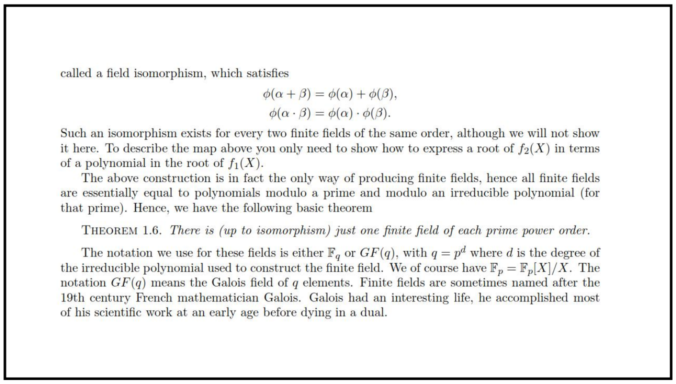
These both consist of the 2^7 binary polynomials of degree less than seven. Addition in these two fields is identical in that one just adds the coefficients of the polynomials modulo two. The only difference is in how multiplication is performed

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

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

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

17



called a field isomorphism, which satisfies

$$\phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta),$$
$$\phi(\alpha \cdot \beta) = \phi(\alpha) \cdot \phi(\beta).$$

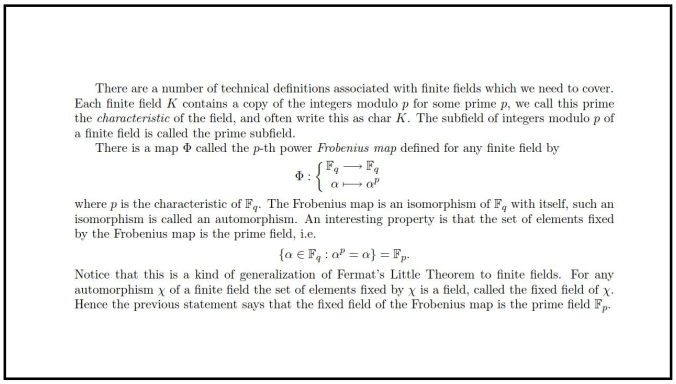
Such an isomorphism exists for every two finite fields of the same order, although we will not show it here. To describe the map above you only need to show how to express a root of $f_2(X)$ in terms of a polynomial in the root of $f_1(X)$.

The above construction is in fact the only way of producing finite fields, hence all finite fields are essentially equal to polynomials modulo a prime and modulo an irreducible polynomial (for that prime). Hence, we have the following basic theorem

THEOREM 1.6. *There is (up to isomorphism) just one finite field of each prime power order.*

The notation we use for these fields is either $\mathbb{F}_q$ or $GF(q)$, with $q = p^d$ where d is the degree of the irreducible polynomial used to construct the finite field. We of course have $\mathbb{F}_p = \mathbb{F}_p[X]/X$. The notation $GF(q)$ means the Galois field of q elements. Finite fields are sometimes named after the 19th century French mathematician Galois. Galois had an interesting life, he accomplished most of his scientific work at an early age before dying in a dual.

18



There are a number of technical definitions associated with finite fields which we need to cover. Each finite field K contains a copy of the integers modulo p for some prime p, we call this prime the *characteristic* of the field, and often write this as char K. The subfield of integers modulo p of a finite field is called the prime subfield.

There is a map Φ called the p-th power *Frobenius map* defined for any finite field by

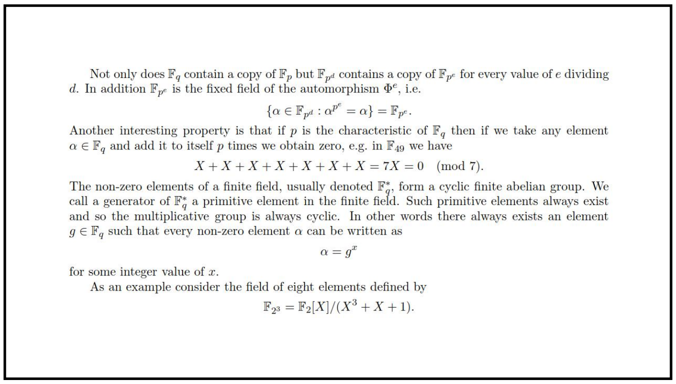
$$\Phi : \begin{cases} \mathbb{F}_q \longrightarrow \mathbb{F}_q \\ \alpha \longmapsto \alpha^p \end{cases}$$

where p is the characteristic of $\mathbb{F}_q$. The Frobenius map is an isomorphism of $\mathbb{F}_q$ with itself, such an isomorphism is called an automorphism. An interesting property is that the set of elements fixed by the Frobenius map is the prime field, i.e.

$$\{\alpha \in \mathbb{F}_q : \alpha^p = \alpha\} = \mathbb{F}_p.$$

Notice that this is a kind of generalization of Fermat's Little Theorem to finite fields. For any automorphism χ of a finite field the set of elements fixed by χ is a field, called the fixed field of χ. Hence the previous statement says that the fixed field of the Frobenius map is the prime field $\mathbb{F}_p$.

19



Not only does $\mathbb{F}_q$ contain a copy of $\mathbb{F}_p$ but $\mathbb{F}_{p^d}$ contains a copy of $\mathbb{F}_{p^e}$ for every value of e dividing d. In addition $\mathbb{F}_{p^e}$ is the fixed field of the automorphism Φ^e, i.e.

$$\{\alpha \in \mathbb{F}_{p^d} : \alpha^{p^e} = \alpha\} = \mathbb{F}_{p^e}.$$

Another interesting property is that if p is the characteristic of $\mathbb{F}_q$ then if we take any element $\alpha \in \mathbb{F}_q$ and add it to itself p times we obtain zero, e.g. in $\mathbb{F}_{49}$ we have

$$X + X + X + X + X + X + X = 7X = 0 \pmod{7}.$$

The non-zero elements of a finite field, usually denoted $\mathbb{F}_q^*$, form a cyclic finite abelian group. We call a generator of $\mathbb{F}_q^*$ a primitive element in the finite field. Such primitive elements always exist and so the multiplicative group is always cyclic. In other words there always exists an element $g \in \mathbb{F}_q$ such that every non-zero element α can be written as

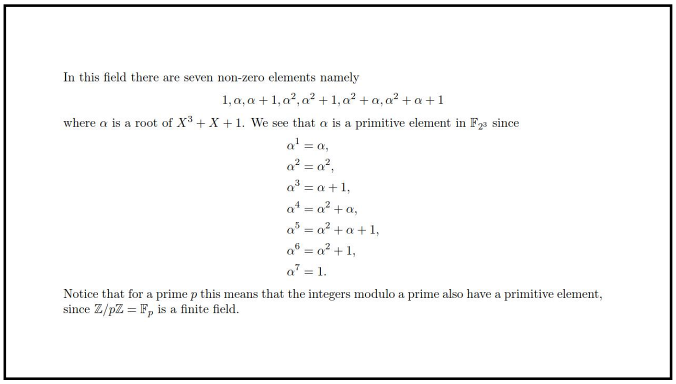
$$\alpha = g^x$$

for some integer value of x.

As an example consider the field of eight elements defined by

$$\mathbb{F}_{2^3} = \mathbb{F}_2[X]/(X^3 + X + 1).$$

20



In this field there are seven non-zero elements namely

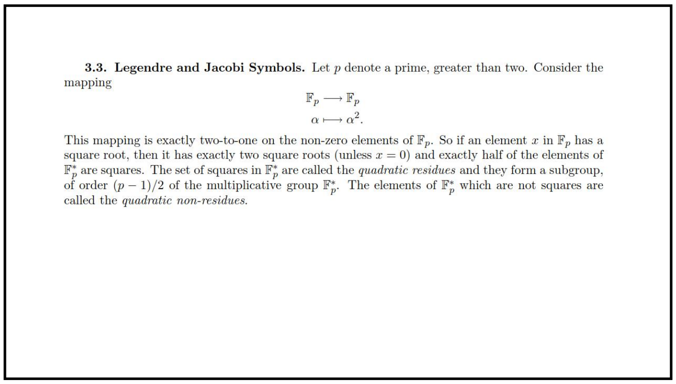
$$1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1$$

where α is a root of $X^3 + X + 1$. We see that α is a primitive element in $\mathbb{F}_{2^3}$ since

$$\begin{aligned} \alpha^1 &= \alpha, \\ \alpha^2 &= \alpha^2, \\ \alpha^3 &= \alpha + 1, \\ \alpha^4 &= \alpha^2 + \alpha, \\ \alpha^5 &= \alpha^2 + \alpha + 1, \\ \alpha^6 &= \alpha^2 + 1, \\ \alpha^7 &= 1. \end{aligned}$$

Notice that for a prime p this means that the integers modulo a prime also have a primitive element, since $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a finite field.

21

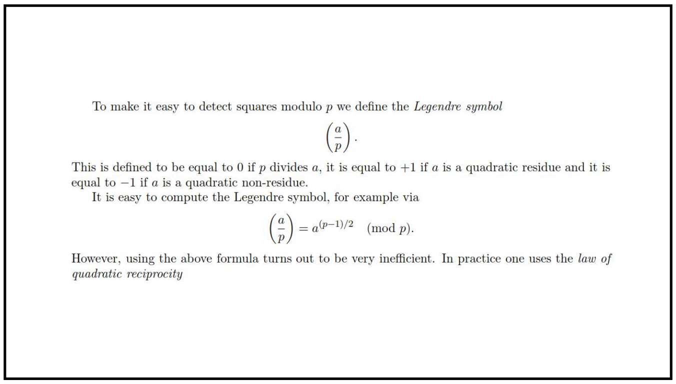


3.3. Legendre and Jacobi Symbols. Let p denote a prime, greater than two. Consider the mapping

$$\begin{aligned} \mathbb{F}_p &\longrightarrow \mathbb{F}_p \\ \alpha &\longmapsto \alpha^2. \end{aligned}$$

This mapping is exactly two-to-one on the non-zero elements of $\mathbb{F}_p$. So if an element x in $\mathbb{F}_p$ has a square root, then it has exactly two square roots (unless $x = 0$) and exactly half of the elements of $\mathbb{F}_p^*$ are squares. The set of squares in $\mathbb{F}_p^*$ are called the *quadratic residues* and they form a subgroup, of order $(p-1)/2$ of the multiplicative group $\mathbb{F}_p^*$. The elements of $\mathbb{F}_p^*$ which are not squares are called the *quadratic non-residues.*

22



To make it easy to detect squares modulo p we define the *Legendre symbol*

$$\left(\frac{a}{p}\right).$$

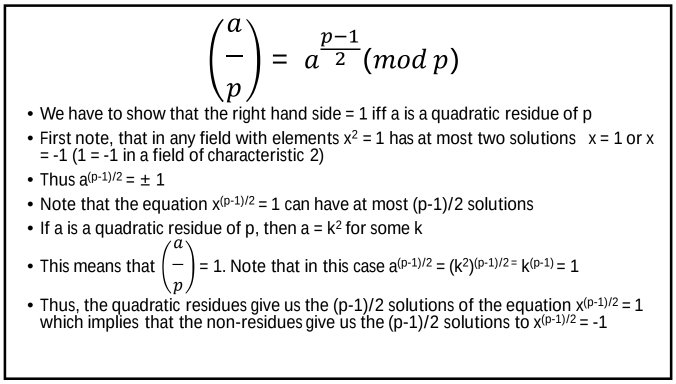
This is defined to be equal to 0 if p divides a, it is equal to $+1$ if a is a quadratic residue and it is equal to -1 if a is a quadratic non-residue.

It is easy to compute the Legendre symbol, for example via

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

However, using the above formula turns out to be very inefficient. In practice one uses the *law of quadratic reciprocity*

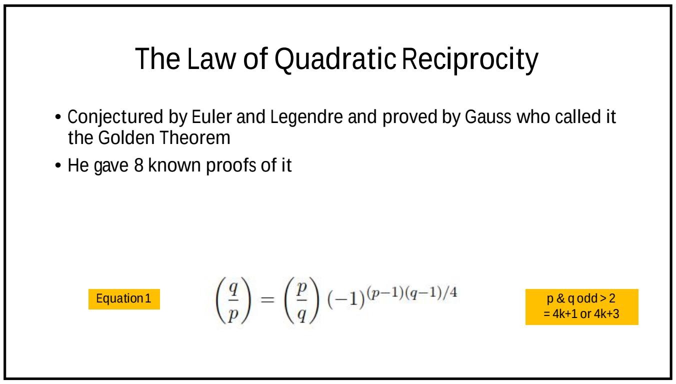
23



$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} (mod\, p)$$

- We have to show that the right hand side = 1 iff a is a quadratic residue of p
- First note, that in any field with elements $x^2 = 1$ has at most two solutions x = 1 or x = -1 (1 = -1 in a field of characteristic 2)
- Thus $a^{(p-1)/2} = \pm 1$
- Note that the equation $x^{(p-1)/2} = 1$ can have at most (p-1)/2 solutions
- If a is a quadratic residue of p, then $a = k^2$ for some k
- This means that $\left(\frac{a}{p}\right)$ = 1. Note that in this case $a^{(p-1)/2} = (k^2)^{(p-1)/2 =} k^{(p-1)} = 1$
- Thus, the quadratic residues give us the (p-1)/2 solutions of the equation $x^{(p-1)/2} = 1$ which implies that the non-residues give us the (p-1)/2 solutions to $x^{(p-1)/2} = -1$

24



The Law of Quadratic Reciprocity

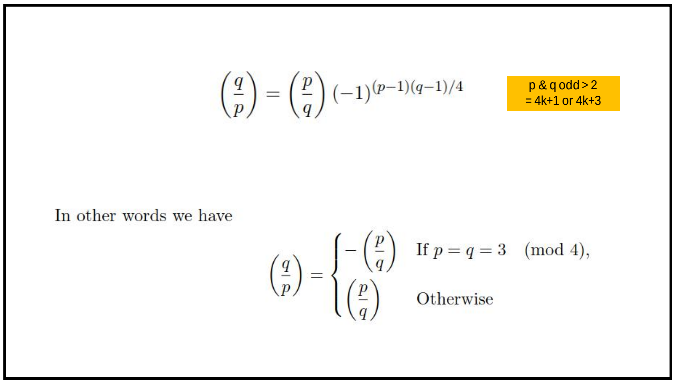
- Conjectured by Euler and Legendre and proved by Gauss who called it the Golden Theorem
- He gave 8 known proofs of it

Equation 1

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4}$$

p & q odd > 2 = 4k+1 or 4k+3

25



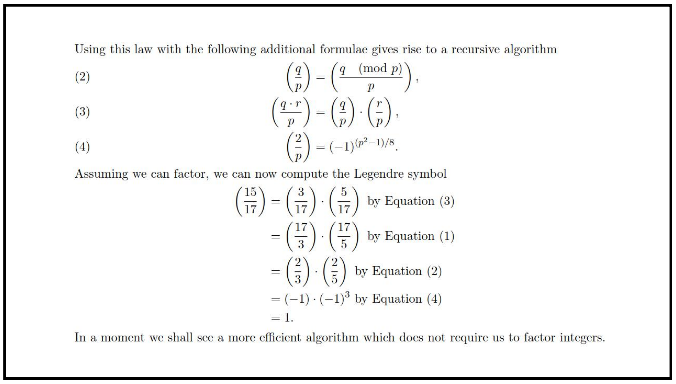
$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4}$$

p & q odd > 2 = 4k+1 or 4k+3

In other words we have

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{If } p = q = 3 \pmod 4, \\ \left(\frac{p}{q}\right) & \text{Otherwise} \end{cases}$$

26



Using this law with the following additional formulae gives rise to a recursive algorithm

(2) $$\left(\frac{q}{p}\right) = \left(\frac{q \pmod p}{p}\right),$$

(3) $$\left(\frac{q \cdot r}{p}\right) = \left(\frac{q}{p}\right) \cdot \left(\frac{r}{p}\right),$$

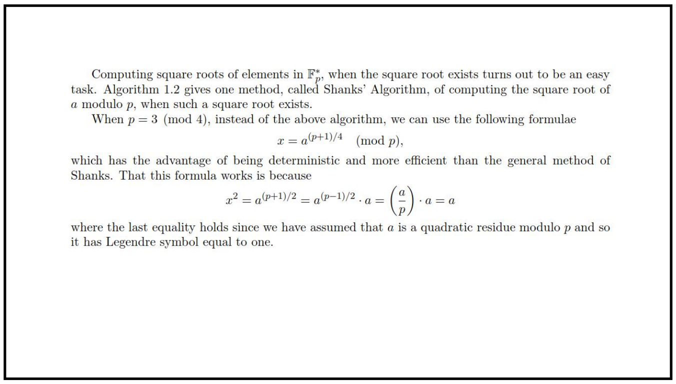
(4) $$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Assuming we can factor, we can now compute the Legendre symbol

$$\begin{aligned} \left(\frac{15}{17}\right) &= \left(\frac{3}{17}\right) \cdot \left(\frac{5}{17}\right) \text{ by Equation (3)} \\ &= \left(\frac{17}{3}\right) \cdot \left(\frac{17}{5}\right) \text{ by Equation (1)} \\ &= \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) \text{ by Equation (2)} \\ &= (-1) \cdot (-1)^3 \text{ by Equation (4)} \\ &= 1. \end{aligned}$$

In a moment we shall see a more efficient algorithm which does not require us to factor integers.

27



Computing square roots of elements in $\mathbb{F}_p^*$, when the square root exists turns out to be an easy task. Algorithm 1.2 gives one method, called Shanks' Algorithm, of computing the square root of a modulo p, when such a square root exists.

When $p = 3 \pmod 4$, instead of the above algorithm, we can use the following formulae

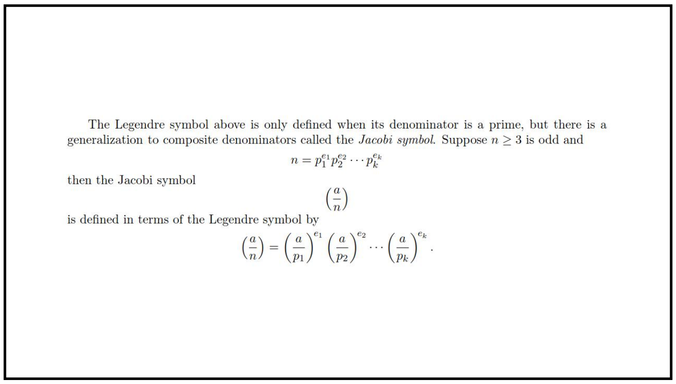
$$x = a^{(p+1)/4} \pmod p,$$

which has the advantage of being deterministic and more efficient than the general method of Shanks. That this formula works is because

$$x^2 = a^{(p+1)/2} = a^{(p-1)/2} \cdot a = \left(\frac{a}{p}\right) \cdot a = a$$

where the last equality holds since we have assumed that a is a quadratic residue modulo p and so it has Legendre symbol equal to one.

28



The Legendre symbol above is only defined when its denominator is a prime, but there is a generalization to composite denominators called the *Jacobi symbol*. Suppose $n \geq 3$ is odd and

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

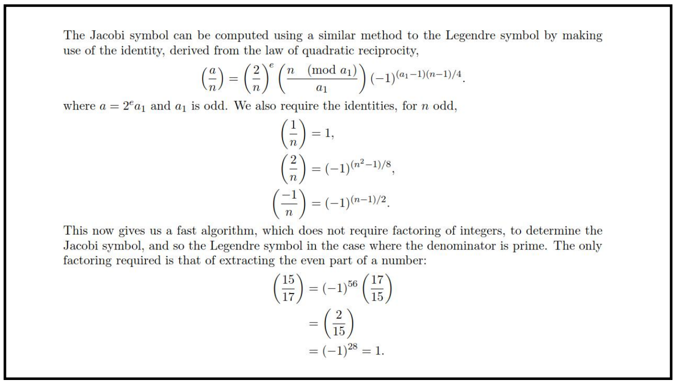
then the Jacobi symbol

$$\left(\frac{a}{n}\right)$$

is defined in terms of the Legendre symbol by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k}.$$

29



The Jacobi symbol can be computed using a similar method to the Legendre symbol by making use of the identity, derived from the law of quadratic reciprocity,

$$\left(\frac{a}{n}\right) = \left(\frac{2}{n}\right)^e \left(\frac{n \pmod{a_1}}{a_1}\right)(-1)^{(a_1-1)(n-1)/4}.$$

where $a = 2^e a_1$ and a_1 is odd. We also require the identities, for n odd,

$$\left(\frac{1}{n}\right) = 1,$$

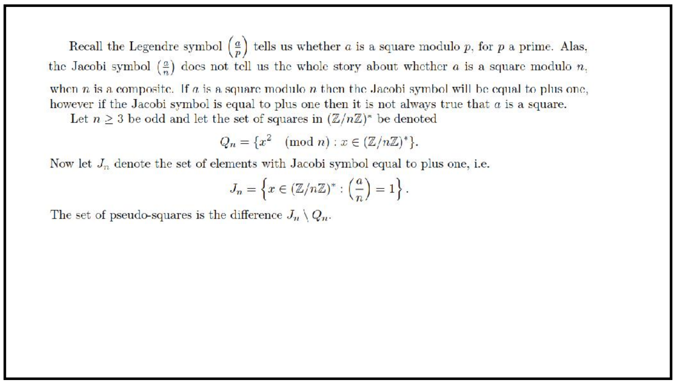
$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8},$$

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}.$$

This now gives us a fast algorithm, which does not require factoring of integers, to determine the Jacobi symbol, and so the Legendre symbol in the case where the denominator is prime. The only factoring required is that of extracting the even part of a number:

$$\begin{aligned} \left(\frac{15}{17}\right) &= (-1)^{56} \left(\frac{17}{15}\right) \\ &= \left(\frac{2}{15}\right) \\ &= (-1)^{28} = 1. \end{aligned}$$

30



Recall the Legendre symbol $\left(\frac{a}{p}\right)$ tells us whether a is a square modulo p, for p a prime. Alas, the Jacobi symbol $\left(\frac{a}{n}\right)$ does not tell us the whole story about whether a is a square modulo n, when n is a composite. If a is a square modulo n then the Jacobi symbol will be equal to plus one, however if the Jacobi symbol is equal to plus one then it is not always true that a is a square.

Let $n \geq 3$ be odd and let the set of squares in $(\mathbb{Z}/n\mathbb{Z})^*$ be denoted

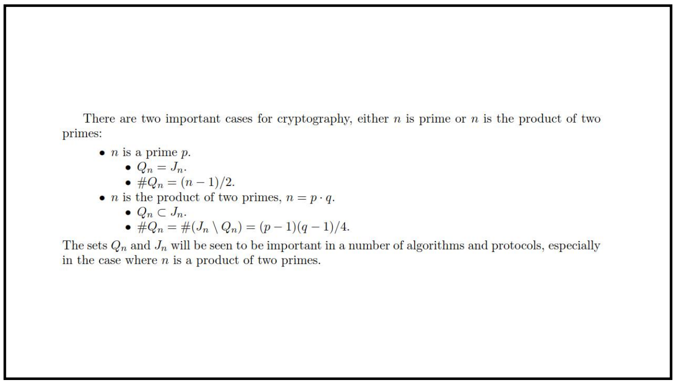
$$Q_n = \{x^2 \pmod n : x \in (\mathbb{Z}/n\mathbb{Z})^*\}.$$

Now let J_n denote the set of elements with Jacobi symbol equal to plus one, i.e.

$$J_n = \left\{x \in (\mathbb{Z}/n\mathbb{Z})^* : \left(\frac{a}{n}\right) = 1\right\}.$$

The set of pseudo-squares is the difference $J_n \setminus Q_n$.

31

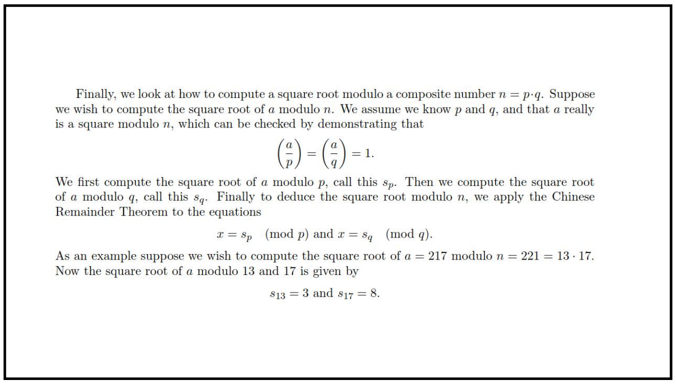


There are two important cases for cryptography, either n is prime or n is the product of two primes:

- n is a prime p.
  - $Q_n = J_n$.
  - $\#Q_n = (n-1)/2$.
- n is the product of two primes, $n = p \cdot q$.
  - $Q_n \subset J_n$.
  - $\#Q_n = \#(J_n \setminus Q_n) = (p-1)(q-1)/4$.

The sets Q_n and J_n will be seen to be important in a number of algorithms and protocols, especially in the case where n is a product of two primes.

32



Finally, we look at how to compute a square root modulo a composite number $n = p \cdot q$. Suppose we wish to compute the square root of a modulo n. We assume we know p and q, and that a really is a square modulo n, which can be checked by demonstrating that

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1.$$

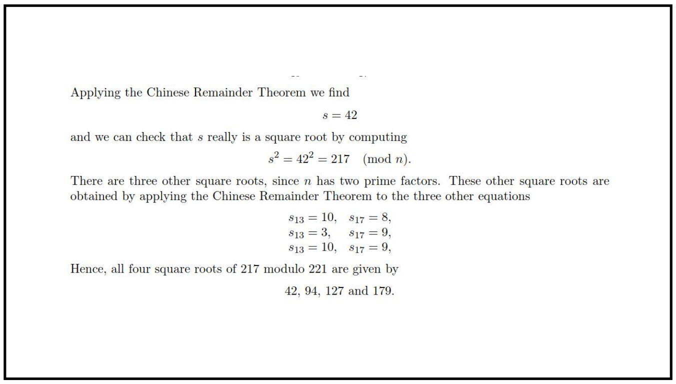
We first compute the square root of a modulo p, call this s_p. Then we compute the square root of a modulo q, call this s_q. Finally to deduce the square root modulo n, we apply the Chinese Remainder Theorem to the equations

$$x = s_p \pmod p \text{ and } x = s_q \pmod q.$$

As an example suppose we wish to compute the square root of $a = 217$ modulo $n = 221 = 13 \cdot 17$. Now the square root of a modulo 13 and 17 is given by

$$s_{13} = 3 \text{ and } s_{17} = 8.$$

33



Applying the Chinese Remainder Theorem we find

$$s = 42$$

and we can check that s really is a square root by computing

$$s^2 = 42^2 = 217 \pmod n.$$

There are three other square roots, since n has two prime factors. These other square roots are obtained by applying the Chinese Remainder Theorem to the three other equations

$$\begin{aligned} s_{13} &= 10, & s_{17} &= 8, \\ s_{13} &= 3, & s_{17} &= 9, \\ s_{13} &= 10, & s_{17} &= 9, \end{aligned}$$

Hence, all four square roots of 217 modulo 221 are given by

$$42, 94, 127 \text{ and } 179.$$

34