Notes for 5 March (Tuesday)

1 The road so far...

1. Proved that the characteristic of fields is 0 or prime.
2. Defined the Frobenius endomorphism for general rings of positive characteristic.

2 A detour into cryptography

It turns out (HW) that any finite field $\mathbb{F}$ has size p^n. Since $\mathbb{F} - \{0\}$ is an Abelian group of size $p^n - 1$, $a^{p^n} = a$ for all $a \in \mathbb{F}$. Using this observation, one can not only construct an example of a finite field of size p^n for all p, n but also prove that any other finite field is isomorphic to one of such constructed examples.

Now we discuss a tiny bit of cryptography (a field that I do not understand). A message is taken to be a string of decimal digits. We want to transmit it securely. Until the 1970s, people used "symmetric encryption algorithms", meaning that the encryption and decryption were done by the same "key" (typically a large, usually, randomly generated prime number). This key was transmitted in a secure way between the sender and the recepient. Obviously this is a problematic idea if the number of recepients is large. The "secure channel" aspect of it was taken care of by the Diffey-Hellman key exchange protocol which is vaguely similar to this problem : Basically, if Bob wants to send an engagement ring to Alice, then he can lock it in a box, and send it. Alice can put her own lock on the box and send it back to Bob. Then Bob can open his lock and send it to Alice. Alice can then open her lock. This is implemented as follows

1. Alice and Bob choose large secret numbers a, b.
2. Alice and Bob agree on two prime numbers g, n which can be kept secret, but it is not necessary (but they must be changed every time).
3. Bob calculates $g^b \ mod \ n$ and sends it to Alice. Alice sends $g^a \ mod \ n$ and sends it to Bob.
4. Then Bob and Alice calculate $(g^a)^b \ mod \ = g^{ab} \ mod \ = (g^b)^a \ mod \ n$. This resulting thing is their shared key. What is being used here is that modular exponentiation can be done quickly but discrete logarithms are hard to find.

But even with this DH way of securely transmitting keys, symmetric cryptography is still inconvenient (what if the keys are changed regularly ?) So "public key" crytography was

developed. Here, everyone can send me encrypted messages (using a public key). But only I can decrypt them using a private key. This asymmetric method is more popular these days. The RSA (Rivest-Shamir-Adleman) public key encryption algorithm works on this basis.

1. Alice chooses large primes p, q and calculates $n = pq$, $\phi(n) = (p-1)(q-1)$.
2. She chooses an integer $e < t$ and coprime with it.
3. She finds the multiplicative inverse d of e in $\mathbb{Z}_t$ (using Bezout's identity).
4. She releases (e, n) as the public key and retains (d, n) as her private key.
5. If you want to send a message $m < n$, then the encrypted message (the "cypher text") is $[c]_n = [m]_n^e$ where $c < n$. It is decrypted as $[m]_n = [c]_n^d$. Indeed, $[c]_n^d = [m]_n^{ed} = [m]_n^{\phi(m)k+1} = [m]_n$ because n is squarefree. This algorithm will be broken if we can find the prime factorisation of an integer efficiently. (Quantum computers can do this.)

3 The Chinese Remainder theorem

Given m, n, a, b, suppose we want to solve a system of congruences, i.e., find an x so that $x \equiv_m a$ and $x \equiv_n b$. This problem was solved by Sunzi in the third century. For instance, find an x so that $x \equiv_3 2$ and $x \equiv_5 3$. To solve this, $x = 3k_1 + 2$ and $x = 5k_2 + 3$. So $3k_1 - 5k_2 = 1$. This can be solved because it is a Diophantine equation and $gcd(3, 5) = 1$. Indeed, $k_1 = 2, k_2 = 1$ is a solution. The general solution is $k_1 = 2 + 5n$, $k_2 = 1 + 3n$. Hence, $x = 8 + 15n$. Likewise, consider $x \equiv_{74} 11$ and $x \equiv_{63} 13$. So $x = 11 + 74k_1 = 13 + 63k_2$. Hence, $2 = 74k_1 - 63k_2$. We shall follow the Extended Euclidean Algorithm : $74 = 63 \times 1 + 11, 63 = 11 \times 6 - 3, 11 = (-3) \times (-3) + 2$. So $2 = -(-3) \times (-3) + 11 = (63 - 11 \times 6) \times 3 + 11 = 63 \times 3 - (74 - 63) \times 17 = 74 \times (-17) + 63 \times 20$. Thus, $k_1 = -17 + 63n$ and $x = 11 + 74 \times (-17) + 63 \times 74n = -1247 + 4662n$. Modulo 63×74 it is unique. More generally, we have the following theorem.

Theorem 1. *Let $m, n > 1$, a, b be integers. Then there is a solution $x = x_0$ of $x \equiv_m a$ and $x \equiv_n b$ iff $gcd(m, n) | b - a$. If x_0 is a solution then the set of all solutions x coincides with the set of x satisfying $x \equiv_{lcm(m,n)} x_0$.*

Proof. $x = b + nk_1 = a + mk_2$. Hence, $b - a = mk_2 - nk_1$ which can be solved iff $gcd(m, n) | b - a$. Suppose $x_0 = b + nk$. Then $x = x_0 + n\frac{m}{gcd(m,n)} \equiv_{lcm(m,n)} x_0$. □

As a corollary, if m, n are coprime, then there is a solution unique upto multiples of mn. Actually, the same principle works for more number of congruences as well.

Theorem 2. *Let $m_1, m_2, \ldots m_n$ be pairwise coprime naturals > 1 and $a_1, \ldots, a_n \in \mathbb{Z}$. Then there is a solution to $x \equiv_{m_i} a_i \; \forall \; i$ that is unique upto multiples of $m_1 m_2 \ldots m_n$.*

Proof. We induct on n ($n = 2$ being done above). Assume truth for $1, 2, 3 \ldots, n-1$. By the induction hypothesis, there exists an x_0 satisfying the first $n - 1$ congruences. The general solution is $x = x_0 + m_1 m_2 \ldots m_{n-1} u$ for all integers u. Now we want to solve

$x_0 + m_1 m_2 \ldots m_{n-1} u = a_n + m_n t$, i.e., $(m_1 \ldots m_{n-1})u - m_n t = a_n - x_0$. Since $m_1 \ldots m_{n-1}$ and m_n are coprime, this equation can be solved with $u = u_0 + m_n h$ where h is any integer. Hence, $x = x_0 + m_1 \ldots m_{n-1} u_0 + m_1 \ldots m_n h$ thus proving the result. $\square$