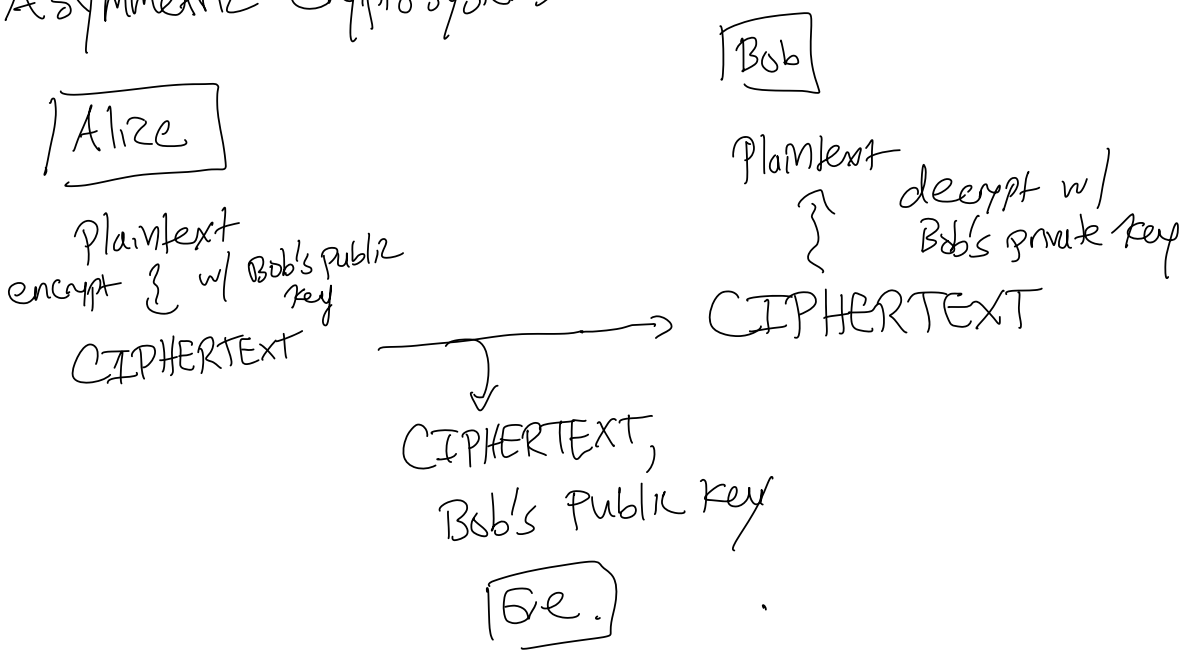
Lecture 2 Divisibility & GCD § 1.2 2022/3/30

Last time Symmetric & Asymmetric Cryptosystems
└ focus of Math 116.

Asymmetric Cryptosystems



converting Private key ⇝ Public key
Should be easy but Public key ⇝ private key
should be hard.

Rmk $P=NP$ would mean that f easy $\Rightarrow f^{-1}$ easy too. If $P=NP$ then public key cryptography would be theoretically impossible.
But everyone thinks $P \neq NP$.

In any case, no public key cryptosystem has been proven to work. They just seem to work in practice.

Ex RSA is based on EASY to multiply
HARD to factor

e.g. $2813 = 29 \times 97$

public key

Ex Diffie-Hellman is based on "discrete log problem".

We will discuss Diffie Hellman before RSA.
But before that, we need some tools from Algebra & Number theory.

Divisibility & GCD §1.2.

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

the integers.

Def Say a divides b, written $a \mid b$, if
$2 \quad -6 \quad 2 \mid -6$

$\exists\, c \in \mathbb{Z}$ s.t. $b = ac$.
$-6 = (2)(-3)$

Def Say d is a common divisor of a & b
$2 \quad -8 \quad 12$

if $d \mid a$ & $d \mid b$.
$2 \mid -8$ & $2 \mid 12$.

Def $\gcd(a, b)$ is the greatest common divisor of a & b.

Goal Today Compute $\gcd(a, b)$ w/ the Euclidean Algorithm.

First: The division algorithm.

Prop 1 (The division algorithm) Given $a, b \in \mathbb{Z}$, $\exists\, q, r \in \mathbb{Z}$ w/ $0 \le r < b$ s.t. $a = qb + r$. □

We leave this w/o proof.

Prop 2 $\gcd(a,b) = \gcd(ax+b, a)$ for any $a, b, x \in \mathbb{Z}$.

Rmk $\begin{pmatrix} ax+b \\ a \end{pmatrix} = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$

& $\det \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} = -1$. We will deduce prop 2 from Prop 4 below.

Prop 3 If $M = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ is any 2×2 matrix of integers, and

$\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$

then $\gcd(v_1, v_2) \mid \gcd(u_1, u_2)$.

Pf $u_1 = xv_1 + yv_2$.

$\gcd(v_1, v_2) \mid u_1$

$\gcd(v_1, v_2) \mid v_1$ & $\gcd(v_1, v_2) \mid \cdots$

$\Rightarrow \gcd(v_1, v_2) \mid x v_1 + y v_2 = u_1$.

Similarly, $\gcd(v_1, v_2) \mid z v_1 + w v_2 = u_2$.

So $\gcd(v_1, v_2)$ divides both u_1 & u_2.

It is a common divisor of u_1 & u_2.

$\gcd(u_1, u_2)$ is the greatest common divisor of u_1 & u_2 $\Rightarrow \gcd(v_1, v_2) \mid \gcd(u_1, u_2)$. $\square$

Prop 4 If M is a 2×2 matrix of integers & $\det(M) = \pm 1$ & $\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = M \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$,

then $\gcd(u_1, u_2) = \gcd(v_1, v_2)$.

Pf By Prop 3, $\gcd(v_1, v_2) \mid \gcd(u_1, u_2)$.

$M^{-1} = \frac{1}{\det M} \begin{pmatrix} w & -y \\ -z & x \end{pmatrix}$ is a matrix of integers too since $\det(M) = \pm 1$.

integers too ...

So $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = M^{-1} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$. & by prop 3 again

$\gcd(u_1, u_2) \mid \gcd(v_1, v_2)$

$\Rightarrow \gcd(u_1, u_2) = \gcd(v_1, v_2)$. ∎

Combining prop 1 & prop 2, we get $\gcd(a,b) = \gcd(b,c)$ where $c < b$.
Repeatedly applying this, eventually we get a decreasing sequence.

Ex $\gcd(20,14)$: $20 = 14 \cdot 1 + 6$

$= \gcd(14,6)$ $\quad 14 = 6 \cdot 2 + 2$

$= \gcd(6,2)$ $\quad 6 = 2 \cdot 3 + 0$

$= \gcd(2,0) = 2$.

Thm (The Euclidean algorithm)

Suppose $a > b$. Let $r_0 = a$ & $r_1 = b$.
Define r_n as the remainder after dividing r_{n-2} by r_{n-1}. (So $r_{n-2} = r_{n-1} \cdot q_n + r_n$)

If $r_{k+1} = 0$ then $r_k = \gcd(a,b)$.
This happens in at most $2\log_2(b) + 2$ steps.

pf See book.

Question For fixed a, b, n when is there a solution to $au + bv = n$?

Ex For which values of n is there a Soln to $20u + 14v = n$?

Observation $\gcd(a,b) \mid a, b$ so it divides $au + bv$ so it must divide n.

If we find a soln to $au + bv = \gcd(a,b)$
We can solve every other Case by Scaling.

Extended Euclidean Algorithm gives a soln to $au+bv = \gcd(a,b)$.

Ex 20, 14.

$20 = 14\cdot 1 + 6 \Rightarrow (1)\ 6 = 20\cdot 1 - 14\cdot 1$

$14 = 6\cdot 2 + 2 \Rightarrow (2)\ 2 = 14 - 6\cdot 2$

Substituting (1) into (2): $2 = 14 - (20\cdot 1 - 14\cdot 1)\cdot 2$

$= 14\cdot 3 - 20\cdot 2.$

So $u = -2$ & $v = 3$ gives a soln to

$20u + 14v = \gcd(20, 14).$

An efficient algorithm:

Idea: Compute a sequence u_i so that for each i, $b \mid (r_i - au_i)$.

Then since $r_k = \gcd(a,b)$, get

$b \mid (r_k - a u_k) = \gcd(a,b) - a u_k$.

Let $\begin{cases} u = u_k \\ v = \dfrac{r_k - a u_k}{b} \end{cases}$.

Then $au + bv = \gcd(a,b)$.

How do we get u_k?

$r_0 = a$ $\quad u_0 = 1$ $\quad b \mid r_0 - a u_0 = 0$

$r_1 = b$ $\quad u_1 = 0$ $\quad b \mid r_1 - a u_1 = b$.

$r_i = r_{i-2} - q r_{i-1}$ $\quad u_i = u_{i-2} - q u_{i-1}$.

Prop For u_i as defined above,
$b \mid r_i - a u_i$ for all i.

Pf By induction. We already checked the base cases, so suppose $b \mid r_{i-2} - a u_{i-2}$

& $b \mid r_{i-1} - a u_{i-1}$. Then

$$r_i - a u_i = (r_{i-2} - q r_{i-1}) - a(u_{i-2} - q u_{i-1})$$

$$= \underbrace{(r_{i-2} - a u_{i-2})}_{b \text{ divides this}} - q \underbrace{(r_{i-1} - a u_{i-1})}_{\& \ b \text{ divides this}}$$

$\Rightarrow b \mid r_i - a u_i$ as desired. $\square$