GTLA Lecture 3, 07.08.2020

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots 2\cdot 1}{k!\,(p-k)(p-k-1)\cdots 2\cdot 1}$$

$$= \frac{p(p-1)\cdots(p-k+2)(p-k+1)(p-k)(p-k-1)\cdots 2\cdot 1}{k!\;\;(p-k)(p-k-1)\cdots 2\cdot 1}$$

$$= \frac{p(p-1)\cdots(p-k+2)(p-k+1)}{k!}$$

RSA Make public (m, e)

(Private: $m = p_1 p_2$
$n = (p_1 - 1)(p_2 - 1)$)

Condition: (for RSA to work) $\gcd(e, n) = 1$

Private: d such that $de = 1$ in $\mathbb{Z}/n\mathbb{Z}$.

$$\text{enc}: \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$
$$x \mapsto x^e$$

$$\text{dec}: \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$
$$y \mapsto y^d$$

RSA works if $(x^e)^d = x$.

<u>Theorem</u> Assume $m = p_1 p_2$, with $p_1, p_2 \in \mathbb{Z}_{>0}$ prime, $p_1 \neq p_2$

$n = (p_1 - 1)(p_2 - 1)$, $\boxed{\gcd(e, n) = 1}$.

Then there exist $d, k \in \mathbb{Z}$ such that

$$de + kn = 1.$$

$x^{ed} = x$, $0^{ed} = 0$

Then $(x^e)^d = x$.

In $\mathbb{Z}/p_1\mathbb{Z}$: $u^{p_1} = u$, $u^{p_1 - 1} = 1$ if $u \neq 0$

<u>Proof</u> (Sketch) In $\mathbb{Z}/p_1\mathbb{Z}$,

$$(x^e)^d = x^{ed} = x^{1-kn} = x(x^{n})^{-k}$$

$$= x\left(x^{(p_1-1)(p_2-1)}\right)^{-k}$$

$$= x\left(1^{p_2-1}\right)^{-k} = x \cdot 1 = x.$$

So $x^{ed} - x = 0$ in $\mathbb{Z}/p_1\mathbb{Z}$.

So p_1 divides $x^{ed} - x$.

Similarly, in $\mathbb{Z}/p_2\mathbb{Z}$, $x^{ed} - x = 0$.

and so p_2 divides $x^{ed} - x$.

Then $p_1 p_2$ divides $x^{ed} - x$.

So $x^{ed}-x=0$ in $\mathbb{Z}/p_1p_2\mathbb{Z}=\mathbb{Z}/m\mathbb{Z}$.

So $x^{ed}=x$ in $\mathbb{Z}/m\mathbb{Z}$

So $(x^e)^d=x$ in $\mathbb{Z}/m\mathbb{Z}$. //

[If
3 divides y
and 5 divides y then 15 divides y.]

<u>Fermat's little theorem</u> $n\in\mathbb{Z}/p\mathbb{Z}$.
If p is prime then in $\mathbb{Z}/p\mathbb{Z}$
$$n^p=n.$$

~~If p is prime and $\Delta=1$ mod~~

<u>Euler's theorem</u> Let p_1,p_2 be prime. ~~If~~ Let $n=(p_1-1)(p_2-1)$.
Let $l=1 \bmod n$. Then
$$x^l=x \text{ in } \mathbb{Z}/p_1p_2\mathbb{Z}.$$

Fields

A field is a number system (commutative ring) such that every nonzero element is invertible.

$\mathbb{Z}/12\mathbb{Z}$ not a field

$\mathbb{Z}/7\mathbb{Z}$ is a field

$\mathbb{Z}/p\mathbb{Z}$ is a field if p is prime.

More fields:

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0 \text{ and } \frac{a}{b} = \frac{c}{d} \text{ if } ad = bc \right\}$$

$$\frac{a}{b} \cdot \frac{b}{a} = 1. \text{ if } \frac{a}{b} \neq \frac{0}{1}.$$

$\mathbb{R} = \{\text{decimal expansions}\}.$

$\mathbb{C} = \{a + bi \mid a \in \mathbb{R}, b \in \mathbb{R}\}$

If $z = a + bi$ then

$$yz = 1 \text{ if } y = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$$

Let $\mathbb{F}$ be a field.

$$\mathbb{F}[x] = \left\{ a_0 + a_1 x + \cdots + a_\ell x^\ell \;\middle|\; \begin{array}{l} \ell \in \mathbb{Z}_{\geq 0} \\ a_1, \ldots, a_\ell \in \mathbb{F} \end{array} \right\}$$

is the number system of <u>polynomials with coefficients in $\mathbb{F}$</u>

<u>Example</u>

(1) $x^2 - 9 \in \mathbb{Q}[x]$

and $(x-3)(x+3) = x^2 - 9$

is a factorization in $\mathbb{Q}[x]$.

$3 \in \mathbb{Q}$ is a solution to $x^2 - 9 = 0$.

$-3 \in \mathbb{Q}$ is a solution to $x^2 - 9 = 0$.

(2) $x^2 - 2 \in \mathbb{Q}[x]$ but <u>does not</u> <u>factor</u>. in $\mathbb{Q}[x]$.

$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

$\sqrt{2} \notin \mathbb{Q}$!!!! This is a factorization in $\mathbb{R}[x]$. (not in $\mathbb{Q}[x]$).

$\Rightarrow$ $\mathbb{Q}$ is not algebraically closed.

Let $\mathbb{F}$ be a field.

$\mathbb{F}$ is <u>algebraically closed</u> if the following holds:

If $x^{\ell}+a_{\ell-1}x^{\ell-1}+\cdots+a_1x+a_0\in\mathbb{F}[x]$

then there exist

$$r_1, r_2, \ldots, r_\ell \in \mathbb{F}$$

such that

$$x^{\ell}+a_{\ell-1}x^{\ell-1}+\cdots a_1x+a_0$$
$$=(x-r_1)(x-r_2)\cdots(x-r_\ell).$$

<u>In English:</u>

$\mathbb{F}$ is algebraically closed if every polynomial in $\mathbb{F}[x]$ factors completely.

Is $\mathbb{R}$ algebraically closed?

<u>NO</u>. Because

$x^2+1\in\mathbb{R}[x]$ but

$x^2+1=(x+i)(x-i)$

and $i\notin\mathbb{R}$ and $-i\notin\mathbb{R}$.

Theorem $\mathbb{C}$ is algebraically closed.

Why should I believe $\sqrt{\pi + e i} \in \mathbb{C}$?? $\sqrt{-1} \notin \mathbb{R}$.

$\sqrt{9} = 3$ since $3^2 = 9$

$\sqrt{9} = -3$ since $(-3)^2 = 9$

and $-3 \neq 3$ even though $\sqrt{9} = \sqrt{9}$.

$\mathbb{Z}/7\mathbb{Z}$ is a field.

Is it algebraically closed?

In $\mathbb{Z}/7\mathbb{Z}$,

$0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 2$

$4^2 = 2$, $5^2 = 4$, $6^2 = 1$

So $\sqrt{0} = 0$, $\sqrt{1} = 1$, $\sqrt{4} = 2$, $\sqrt{2} = 3$

$\sqrt{2} = 4$, $\sqrt{4} = 5$, $\sqrt{1} = 6$

$\sqrt{4} = 2$

$\sqrt{4} = 5$

(should we ban $\sqrt{\ }$??)

Does $x^2-5=0$ have a solution in $\mathbb{Z}/7\mathbb{Z}$?

(Is there $x \in \mathbb{Z}/7\mathbb{Z}$ such that $x^2=5$?)

No.

x^2-5 does not factor in $\mathbb{F}_7[x]$ if $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$.

Common notation:

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ if p is prime.

So $\mathbb{F}_7$ is not algebraically closed.