

Cryptography and Data Security



Number Theory (1 of 2)

(presented by Aleksandr Yampolskiy)

Who is this?



Évariste Galois (1811-1832)

Divisors

- A non-zero number b **divides** a if $\exists m$ s.t. $a=mb$ ($a,b,m \in \mathbf{Z}$)
- That is, b divides into a with no remainder
- We denote this $b|a$
- Example:
 - all of 1,2,3,4,6,8,12,24 divide 24
 - $6 | 24$ ($4 \cdot 6 = 24$), $1 | 24$ ($24 \cdot 1 = 24$), but $5 \nmid 24$ (no $m \in \mathbf{Z}$ such that $m \cdot 5 = 24$)

Divisors (cont.)

- Some axioms:
 - $a|1 \Rightarrow a = \pm 1$
 - $a|b \wedge b|a \Rightarrow a = \pm b$
 - $\forall b \neq 0, b|0$
 - $b|g \wedge b|h \Rightarrow b|(mg + nh)$
- A number p is prime, $p \neq 1 \wedge \forall m \in \mathbb{Z}$
 $(1, p) \mid m \nmid p$

Groups

- **Def:** A set G with a binary operation $?$: $G \times G \rightarrow G$ is called a **group** if:
 1. (closure) $\forall a, b \in G, a ? b \in G$
 2. (associativity) $\forall a, b, c \in G, (a ? b) ? c = a ? (b ? c)$
 3. (identity element) $\exists e \in G, \forall a \in G, a ? e = a$
 4. (inverse element) $\forall a \in G, \exists a^{-1} \in G, a ? (a^{-1}) = e$
- A group is commutative (**Abelian**) if $\forall a, b \in G, a ? b = b ? a$

Examples of groups

- Integers under addition, $(\mathbb{Z}, +) = \{\dots, -2, -1, 0, +1, +2, \dots\}$.
Identity: $e = 0$. Inverses: $a^{-1} = -a$
- $(\{\text{Britney}, \text{Dustin}\}, ?)$, where
 - Britney? Britney = Britney
 - Britney? Dustin = Dustin
 - Dustin ? Britney = Dustin
 - Dustin ? Dustin = BritneyIdentity: $e = \text{Britney}$. Inverses: $\text{Britney}^{-1} = \text{Britney}$, $\text{Dustin}^{-1} = \text{Dustin}$.

Subgroups

- Let $(G, ?)$ be a group. $(H, ?)$ is a **sub-group** of $(G, ?)$ if it is a group, and $H \subseteq G$.
- **Lagrange's theorem**: if G is **finite** and $(H, ?)$ is a sub-group of $(G, ?)$ then $|H|$ **divides** $|G|$

Cyclic groups

- We define **exponentiation** as repeated application of operator \cdot . For example,
 - $a^3 = a \cdot a \cdot a$
 - we also define $a^0 = e$ and $a^{-n} = (a^{-1})^n$
- A group G is **cyclic** if every element is a power of some fixed element.
- That is, $G = \langle a \rangle = \{e, a, a^2, a^3, \dots\}$ for some a .
- a is said to be a generator of the group



A theorem...



Theorem: If $(G, ?)$ is a finite group, then
 $a^{|G|} = e$.

Proof:

- Fix $a \in G$. Consider $\langle a \rangle = \{a^0 = e, a, a^2, \dots\}$
- $|G| < \infty \wedge \langle a \rangle = G \implies |\langle a \rangle| < \infty$
- Hence, $\langle a \rangle = \{e, a, a^2, \dots, a^{k-1}\}$ for some k and $a^k = e$.
- By Lagrange's Theorem, $|\langle a \rangle|$ divides $|G| \implies |G| = d|\langle a \rangle|$ for some $d \in \mathbb{Z}$.
- So, $a^{|G|} = a^{d|\langle a \rangle|} = a^{dk} = \{a^k\}^d = e^d$. QED.

Rings

- **Def:** A set R together with two operations $(+, ?)$ is a **ring** if
 1. $(R, +)$ is an Abelian group.
 2. $(R, ?)$ is a semi-group (just needs to be associative)
 3. $?$ distributes over $+$: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$
- We use $+$, $?$, only for the sake of using familiar and intuitive notation. We could instead use any symbols. We are NOT doing regular addition/multiplication.
- In the ring R , we denote by: $-a$, the additive inverse of a . On commutative rings, the multiplicative inverse of a is denoted by a^{-1} (when it exists).

Rings (cont.)

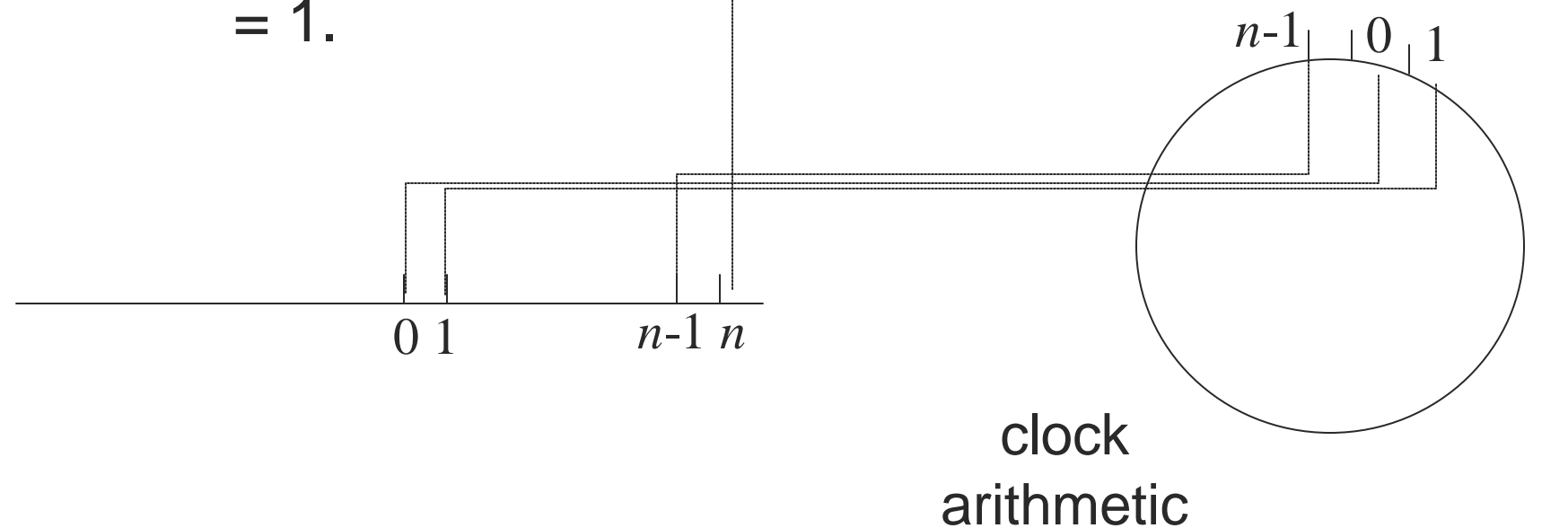
- Example: set of 2×2 matrices forms a ring under regular matrix $(+, *)$.
- Some questions to think about:
 - Is it always the case that $A + B = B + A$?
 - What about $A * B = B * A$?
 - What is the identity element?

Fields

- **Def:** A field is a commutative ring with identity where each non-zero element has a **multiplicative inverse**: $\forall a \neq 0 \in F, \exists a^{-1} \in F, a \cdot a^{-1} = 1$
- Equivalently, $(F, +)$ is a commutative (**additive**) group and $(F \setminus \{0\}, \cdot)$ is a commutative (**multiplicative**) group.
- **Example:** set of rational numbers \mathbf{Q}

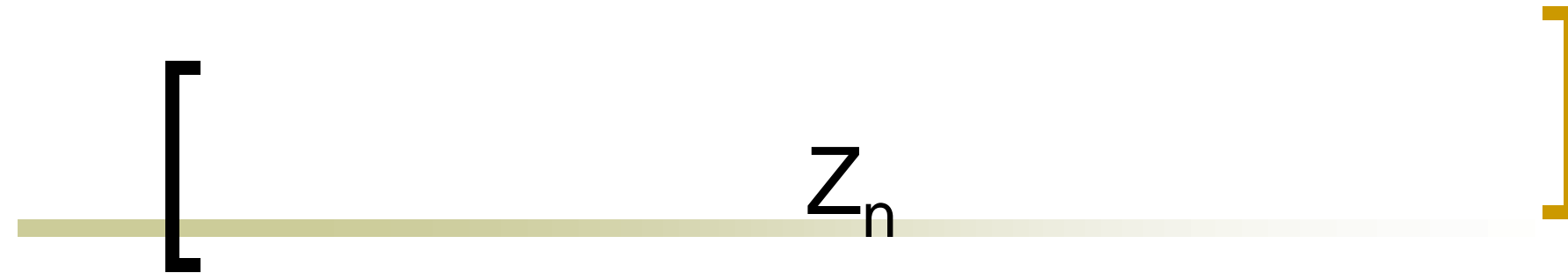
Modular arithmetic

- **Def:** Modulo operator $a \bmod n$ = remainder when a is divided by n
(Another notation: $a \% n$)
- **Example:** $11 \bmod 7 = 4$, $10 \bmod 5 = 0$, $3 \bmod 2 = 1$.



Modular arithmetic (cont.)

- a is **congruent** to b ($a = b \pmod n$) if when divided by n , a and b give the same remainder ($a \pmod n = b \pmod n$)
- $a \sim b \pmod n$ if $n \mid (a - b)$
- E.g. $100 \sim 34 \pmod{11}$



- $a \sim b \pmod n$ defines an equivalence relation
- **set of residues** $Z_n = \{0, 1, \dots, n-1\}$
- Each integer $r \in Z_n$ actually represents a **residue class** $[r] = \{a \in \mathbf{Z} : a \sim r \pmod n\}$

[

Z_n (cont.)

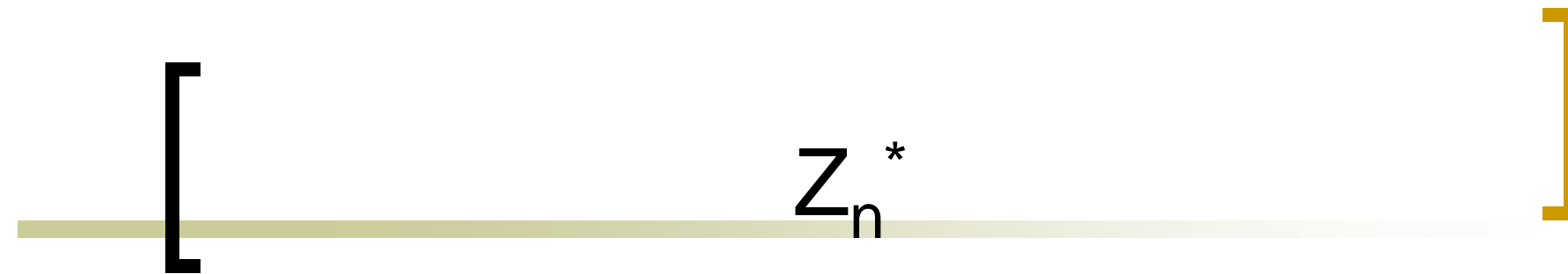
]

E.g., $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$. But in fact, we are dealing with:

...						
-21	-20	-19	-18	-17	-16	-15
-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34
...						

Z_n (cont.)

- Integers mod n $Z_n = \{0, 1, \dots, n-1\}$ is an Abelian group.
- **Example:** What is $3+5$ in Z_7 ? What is -6 in Z_7 ?
- Note some peculiarities for Z_n
 - if $(a+b)=(a+c) \pmod n$ then $b=c \pmod n$
 - but $(ab)=(ac) \pmod n$ then $b=c \pmod n$ only if a is relatively prime to n



- **Multiplicative integers mod n**
 $Z_n^* = \{x \in Z_n : \gcd(x, n) = 1\}$
- Z_n^* consists of all integers $0 \dots n-1$ relatively prime with n
- What is the size of this group? **Euler's totient function** $\phi(n) = |Z_n^*|$

Z_n^* (cont.)

- What is $\phi(p)$ when p is prime?
 - $Z_p^* = \{1, 2, \dots, p-1\}$) $\phi(p) = |Z_p^*| = p - 1$.
- What about $\phi(p^k)$ where p is prime and $k > 1$?
 - $Z_{p^k} = \{0, 1, \dots, p^k - 1\}$
 - How many multiples of p are in Z_{p^k} ?
 - Multiples are $\{0, p, 2p, \dots, (p^{k-1} - 1)p\}$. There are p^{k-1} of them
 - Hence, $\phi(p^k) = p^k - p^{k-1}$

Z_n^* (cont.)

- $\phi(mn) = \phi(m)\phi(n)$
- $\phi(\prod_i p_i^e) = \prod_i (p_i^e - p_i^{e-1})$
- **Example:**
 - $\phi(10) = \phi(2)\phi(5) = 1\phi(4) = 4$
 - $S = \{1 \cdot n \cdot 10 : n \text{ relatively prime to } 10\} = \{1, 3, 7, 9\}$. Notice that $|S| = 4$ as expected.



To be continued next time...