The wonderful world of arithmetic

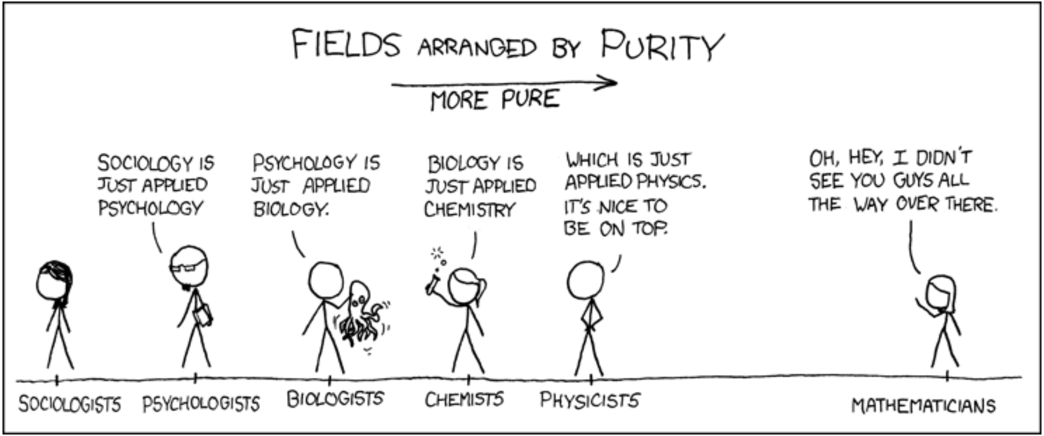
And its applications to cryptography

Karst Koymans

Informatics Institute
University of Amsterdam
(version 24.6, 2024/09/25 11:51:30 UTC)

Thursday, September 26, 2024

Mathematicians



Source: `https://xkcd.com/435/`

Outline of Part I

1. Numbers and basic arithmetic laws
   - Commutative monoids and groups
   - Combining addition and multiplication
   - Primes
   - Greatest common divisor
2. Arithmetic in finite structures
   - Modular arithmetic
   - Euler's φ
   - Chinese Remainder Theorem
3. Applications to cryptography
   - RSA
   - Diffie-Hellman

Outline of Part II

4. Calculating with polynomials
   - Polynomials over a general field
   - Polynomials over $\mathbb{Z}_p$
5. Finite fields
   - Galois fields
   - Application to AES(Rijndael)

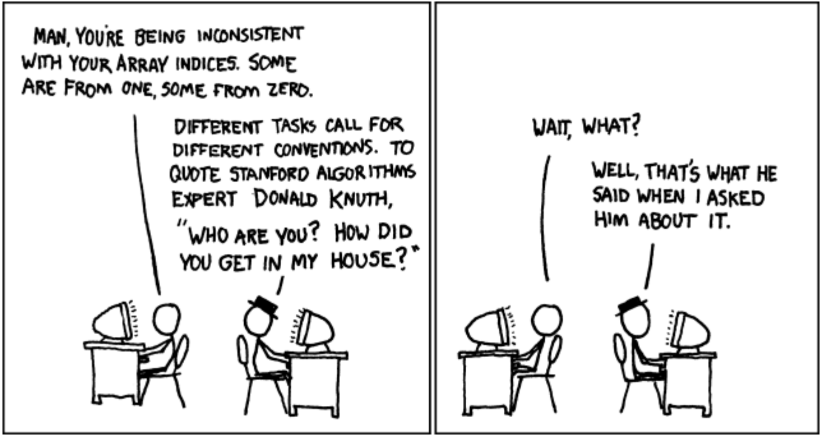
Outline of Part III

Part I

Basic math

Outline

The role of zero



Source: `https://xkcd.com/163/`

Also see: `https://www.explainxkcd.com/wiki/index.php/163:_Donald_Knuth`

Outline

1. Numbers and basic arithmetic laws
   - Commutative monoids and groups
   - Combining addition and multiplication
   - Primes
   - Greatest common divisor
2. Arithmetic in finite structures
3. Applications to cryptography

The natural numbers

Properties of (commutative) monoids

$$\mathbb{N} =< \{0, 1, 2, \ldots\}, +, 0 >$$

Laws

$$\forall x \forall y (x + y = y + x) \qquad \text{(Commutativity)}$$

$$\forall x \forall y \forall z ((x + y) + z = x + (y + z)) \qquad \text{(Associativity)}$$

$$\forall x (x + 0 = x) \qquad \text{(Neutral element)}$$

Non-law

$$\forall x \exists y (x + y = 0) \qquad \text{(Existence of inverses)}$$

The integers

Properties of (commutative) groups

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

Laws

$$\forall x \forall y (x + y = y + x) \quad \text{(Commutativity)}$$

$$\forall x \forall y \forall z ((x + y) + z = x + (y + z)) \quad \text{(Associativity)}$$

$$\forall x (x + 0 = x) \quad \text{(Neutral element)}$$

$$\forall x \exists y (x + y = 0) \quad \text{(Existence of inverses)}$$

Abelian (commutative) groups

An axiomatisation

$$\mathbb{G} = < G, \star, e, (\cdot)^{-1} >$$

Laws

$$\forall x \forall y (x \star y = y \star x) \qquad \text{(Commutativity)}$$

$$\forall x \forall y \forall z ((x \star y) \star z = x \star (y \star z)) \qquad \text{(Associativity)}$$

$$\forall x (x \star e = x) \qquad \text{(Neutral element)}$$

$$\forall x (x \star x^{-1} = e) \qquad \text{(Existence of inverses)}$$

Because inverses are provably unique the existential quantifier can be turned into a unary function.

Examples

and non-examples

Examples (No groups)

$$< \mathbb{Z}, \cdot, 1 >$$

$$< \mathbb{Q}, \cdot, 1 >, \text{with } \mathbb{Q} = \{\frac{p}{q} | p, q \in \mathbb{Z}, q \neq 0\}$$

Examples (Groups)

$$\mathbb{Q}^* =< \mathbb{Q}\backslash\{0\}, \cdot, 1 >$$

$$\mathbb{R}^* =< \mathbb{R}\backslash\{0\}, \cdot, 1 >$$

$$\mathbb{C}^* =< \mathbb{C}\backslash\{0\}, \cdot, 1 >$$

Here $\mathbb{R}$ is the set of reals $(\sqrt{2}, e, \pi, \ldots)$
and $\mathbb{C}$ is the set of complex numbers adding $i = \sqrt{-1}$.

Outline

The field of rational numbers

Groups

$$\mathbb{Q} =< \mathbb{Q}, +, 0 >$$

$$\mathbb{Q}^* =< \mathbb{Q}\backslash\{0\}, \cdot, 1 >$$

can be combined into

A field

$$\mathbb{Q} =< \mathbb{Q}, +, \cdot, 0, 1 >$$

defining the **field** of rational numbers.

General fields

and their axiomatisation

A field $< F, \oplus, \star, 0, 1 >$ consists of

- A commutative group $< F, \oplus, 0 >$
- and a commutative group $< F \backslash \{0\}, \star, 1 >$
- satisfying

Distributivity

$$\forall x \forall y \forall z ((x \oplus y) \star z = (x \star z) \oplus (y \star z)) \qquad \text{(Distributivity)}$$

- but never satisfying

"Wrong" distributivity

$$\forall x \forall y \forall z ((x \star y) \oplus z = (x \oplus z) \star (y \oplus z)) \qquad \text{(Wrong distributivity)}$$

Outline

Primes

and unique factorisation

$$\begin{aligned} \mathbb{P} &= \{2, 3, 5, 7, 11, 13, \ldots\} \\ &= \{p_0, p_1, p_2, p_3, p_4, p_5, \ldots\} \end{aligned}$$

So $p_0 = 2, p_1 = 3, p_2 = 5, \ldots$ in increasing order.

Theorem

Every natural number $n > 0$ can be written in an essentially unique way as a product of primes:

$$n = \prod_{i=0}^{k-1} p_i^{a_i}$$

for some natural number k, where $a_{k-1} > 0$ if $k > 0$.

Example prime factorisations

Example

$$210 = 2 \cdot 3 \cdot 5 \cdot 7 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1 = p_0^1 \cdot p_1^1 \cdot p_2^1 \cdot p_3^1$$

Example

$$189 = 3 \cdot 3 \cdot 3 \cdot 7 = 2^0 \cdot 3^3 \cdot 5^0 \cdot 7^1 = p_0^0 \cdot p_1^3 \cdot p_2^0 \cdot p_3^1$$

These factorisations give an isomorphism $\mathbb{N}_{>0} \cong \bigoplus_\omega \mathbb{N}$, where

$$\bigoplus_\omega \mathbb{N} = \{< e_0, e_1, \ldots > \mid e_i = 0 \text{ for all but finitely many } i \in \mathbb{N}\}.$$

Outline

Greatest common divisor

An example of Euclid's algorithm

We want to find the gcd (greatest common divisor) of 49 and 35:

Euclid's reduction (instance of Euclid's algorithm)

$$49 = 1 \cdot 35 + 14 \implies \text{gcd}(49, 35) = \text{gcd}(35, 14)$$

$$35 = 2 \cdot 14 + 7 \implies \text{gcd}(35, 14) = \text{gcd}(14, 7)$$

$$14 = 2 \cdot 7 + 0 \implies \text{gcd}(14, 7) = \text{gcd}(7, 0) = 7$$

Euclid's reversal (extended Euclid's algorithm)

$$7 = 35 - 2 \cdot 14 \quad \wedge \quad 14 = 49 - 1 \cdot 35$$

$$\begin{aligned} 7 &= 35 - 2 \cdot (49 - 1 \cdot 35) \\ &= -2 \cdot 49 + 3 \cdot 35 \end{aligned}$$

Extended Euclidean algorithm in compact table format

Greatest common divisor of 49 and 35

	49	35									
49	1	0	49	$=$	1	$\cdot$	49	$+$	0	$\cdot$	35
35	0	1	35	$=$	0	$\cdot$	49	$+$	1	$\cdot$	35
14	1	-1	14	$=$	1	$\cdot$	49	$+$	-1	$\cdot$	35
7	-2	3	7	$=$	-2	$\cdot$	49	$+$	3	$\cdot$	35

Greatest common divisor

Euclid's algorithm

Theorem

For all $a, b \in \mathbb{Z}$ we can (effectively) find $p, q \in \mathbb{Z}$ such that

$$gcd(a, b) = p \cdot a + q \cdot b$$

Finding p and q can be done using the extended Euclid's algorithm.

Definition

a and b are called relatively prime iff $\gcd(a, b) = 1$.

Theorem

If a and b are relatively prime the extended Euclid's algorithm calculates p and q such that

$$p \cdot a + q \cdot b = 1$$

Outline

1. Numbers and basic arithmetic laws
2. Arithmetic in finite structures
   - Modular arithmetic
   - Euler's φ
   - Chinese Remainder Theorem
3. Applications to cryptography

Outline

Clock arithmetic

$24 = 0$ (or maybe $12 = 0$)

- $\mathbb{Z}_{24} = \{0, 1, 2, \ldots, 23\}$
- $23 + 1 \equiv 24 \equiv 0 \pmod{24}$

Definition ($a, b, n \in \mathbb{Z}$, usually with $n > 1$)

$a \equiv b \pmod{n} \iff n \mid (a - b) \iff \exists k \in \mathbb{Z}(k \cdot n = (a - b))$

Theorem

"$\equiv \pmod{n}$" is an equivalence relation on $\mathbb{Z}$ which is also happens to be a congruence. $\mathbb{Z}_n$ is a standard representing set of the integers modulo n.

Corollary

Addition and multiplication can be performed $\pmod{n}$ as usual.

Clock arithmetic

Examples

Examples

$$22 + 5 \equiv 3 \pmod{24}$$

$$22 \cdot 5 \equiv 110 \equiv 14 \pmod{24}$$

$$-2 \cdot 5 \equiv -10 \equiv 14 \pmod{24}$$

$$2 \cdot 12 \equiv 24 \equiv 0 \pmod{24}$$

$$2 \not\equiv 0 \pmod{24}$$

$$12 \not\equiv 0 \pmod{24}$$

$\mathbb{Z}_{24}$ has "divisors of zero" or "zero divisors".
This is considered an unwanted property in general.

Clock arithmetic

The modulo function (% in Ruby or Python)

The function $(.) \pmod{n}$, for a given $n > 0$

The notation $a \pmod{n}$ means the unique b with $0 \leq b < n$ and $a \equiv b \pmod{n}$.
Hence $(.) \pmod{n} : \mathbb{Z} \to \mathbb{Z}_n$.

Examples

$$3 \pmod{7} = 3$$

$$13 \pmod{7} = 6$$

$$-3 \pmod{7} = 4$$

$$21 \pmod{7} = 0$$

$$a \pmod{n} \equiv a \pmod{n}$$

Who's afraid of zero?

or the AM/PM mess

- Splitting up 24 hours as $2 \cdot 12$ hours the sensible way:
  - 0:00 AM (midnight), 1:00 AM, ..., 11:59 AM
  - 0:00 PM (midday, noon), 1:00 PM, ..., 11:59 PM
- Splitting up 24 hours as $2 \cdot 12$ hours the confusing way:
  - 12:00 AM (midnight), 12:59 AM, 1:00 AM, ..., 11:59 AM
  - 12:00 PM (midday, noon), 12:59 PM, 1:00 PM, ..., 11:59 PM
  - $12 \equiv 0 \pmod{12}$, but $12 \not\equiv 0 \pmod{24}$,

    so using 12 hours in this context is confusing
    - For instance in Japan 00:00 AM is midnight and 12:00 AM is noon

Multiplication tables

for $\mathbb{Z}_n\backslash\{0\}$

Example ($\mathbb{Z}_5\backslash\{0\}$)

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Example ($\mathbb{Z}_6\backslash\{0\}$)

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Again, working modulo 6 gives these nasty zero divisors,
but working modulo 5 (a prime) seems to behave much better.

Prime fields

Theorem

$\mathbb{F}_p =< \mathbb{Z}_p, +, \cdot, 0, 1 >$ *is a field if and only if p is prime.*
$\mathbb{Z}_n^* =< \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}, \cdot, 1 >$ *is a group for all* $n \in \mathbb{N}, n > 1$.

Example ($\mathbb{Z}_{12}^*$)

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Example ($\mathbb{Z}_{10}^*$)

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Note that these groups have the same number of elements
but are not isomorphic!

Outline

1. Numbers and basic arithmetic laws
2. Arithmetic in finite structures
   - Modular arithmetic
   - Euler's φ
   - Chinese Remainder Theorem
3. Applications to cryptography

Euler's φ-function

and the Euler-Fermat theorem

Definition ($n \in \mathbb{N}, n > 1$)

$\varphi(n)$ is the number of elements of $\mathbb{Z}_n^*$:

$$\varphi(n) = |\mathbb{Z}_n^*|$$

Theorem

For all $a \in \mathbb{Z}_n^*$ (or in other words gcd(a, n) = 1)

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Example

$$\varphi(10) = 4$$

$$\varphi(12) = 4$$

More properties of Euler's φ-function

Theorem

$\varphi(p^k) = p^{k-1}(p-1)$, for all primes p and $k > 0$.
In particular $\varphi(p) = p - 1$, for all primes p ($k = 1$).
$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, for all relatively prime m and n.

Examples

$$\varphi(18) = \varphi(2 \cdot 3^2) = \varphi(2) \cdot \varphi(3^2) = (2-1) \cdot 3^{(2-1)} \cdot (3-1) = 1 \cdot 3^1 \cdot 2 = 6$$

$$\varphi(125) = \varphi(5^3) = 5^2 \cdot 4 = 100$$

Corollary

If p and q are different primes and $N = pq$, then $\varphi(N) = (p-1)(q-1)$.

Cyclicity properties of $\mathbb{Z}_n^*$

Example ($\mathbb{Z}_8^*$ is not cyclic)

$$3^1 = 3; 3^2 = 1$$

$$5^1 = 5; 5^2 = 1$$

$$7^1 = 7; 7^2 = 1$$

All elements except 1 have order 2.

Theorem

$\mathbb{Z}_p^*$ is cyclic of order $p-1$ for all primes p.
For every prime p we have at least one isomorphism

$$< \mathbb{Z}_{p-1}, +, 0 > \cong < \mathbb{Z}_p^*, \cdot, 1 >$$

Warning

These isomorphisms are easy to calculate from left to right
but hard from right to left!

Multiplicative order and primitive roots

Example ($\mathbb{Z}_7^*$ is cyclic of the maximal order 6)

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

$$3^0 = 1; 3^1 = 3; 3^2 = 2; 3^3 = 6; 3^4 = 4; 3^5 = 5; 3^6 = 1$$

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

$$5^0 = 1; 5^1 = 5; 5^2 = 4; 5^3 = 6; 5^4 = 2; 5^5 = 3; 5^6 = 1$$

$$6^0 = 1; 6^1 = 6; 6^2 = 1$$

3 and 5 are primitive roots of order 6.

2 and 4 have order 3, while 6 has order 2.

$$< \mathbb{Z}_6, +, 0 > \cong < \mathbb{Z}_7^*, \cdot, 1 > \text{, using } x \mapsto 3^x \text{ or } x \mapsto 5^x$$

.

Outline

Chinese Remainder Theorem

Theorem

Whenever $n_1, \ldots, n_k \in \mathbb{N}_{>1}$ *are pairwise relatively prime*
we can solve the simultaneous set of n congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\ldots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

The solution x *is unique* $(\mathrm{mod}\ n_1 \cdot \ldots \cdot n_k)$.
This can also be stated as

$$\mathbb{Z}_{n_1 \cdot \ldots \cdot n_k} \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$$

Simple example for the CRT

Example ($\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$)

$\mathbb{Z}_{12}$	$\mathbb{Z}_3$	$\mathbb{Z}_4$
0	0	0
1•	1•	1•
2	2•	2
3	0	3•
4	1•	0
5•	2•	1•
6	0	2
7•	1•	3•
8	2•	0
9	0	1•
10	1•	2
11•	2•	3•

Euler's function special case

Product of two primes

Theorem

Let $p, q \in \mathbb{P}$ be two primes ($p \neq q$) and let $n = pq$.

$$
\begin{array}{rcl}
\mathbb{Z}_n & \cong & \mathbb{Z}_p \times \mathbb{Z}_q \\
\mathbb{Z}_n^* & \cong & \mathbb{Z}_p^* \times \mathbb{Z}_q^* \\
\varphi(n) & = & \varphi(p)\varphi(q) \\
\varphi(p) & = & p - 1 \\
\varphi(q) & = & q - 1
\end{array}
$$

In general $\varphi(n)$ is difficult to calculate, but for $n = pq$, where p and q are known primes, this is easy: $\varphi(n) = (p-1)(q-1)$.

Outline

Outline

RSA (Textbook variant)

Its definition

Definition (RSA)

RSA works with public information (Uppercase,blue) and private information (lowercase,red).

- A public modulus $N = pq$, which is the product of two private (secret) primes. Notice that $\varphi(N) = (p-1)(q-1)$, which is (as far as we know) hard to calculate if you do not know the primes p and q.
- A public exponent $E \in \mathbb{Z}^*_{\varphi(N)}$.
- A private exponent d such that $Ed \equiv 1 \pmod{\varphi(N)}$. d can easily be calculated using Euclid's algorithm.
- (N, E) is called the public key.
- $(p, q = \frac{N}{p}, d)$ is called the private key.
- $(N = pq, E, d)$ is called a public/private key "pair".

RSA (Textbook variant)

Its principle of operation

Theorem

A message is represented as a positive $m < N$. This message is encrypted as $C = m^E \pmod{N}$. Then decryption follows from $m \equiv C^d \pmod{N}$.

Proof.

Let $C = m^E \pmod{N}$ and $Ed = 1 + k\varphi(N)$.
Then

$$\begin{aligned} C^d &\equiv (m^E)^d \pmod{N} \equiv m^{Ed} \pmod{N} \\ &\equiv m^{(1+k\varphi(N))} \pmod{N} \\ &\equiv m(m^{\varphi(N)})^k \pmod{N} \\ &\equiv m1^k \pmod{N} \equiv m \pmod{N} \end{aligned}$$

Who spots the (minor) omission in this proof? □

Outline

Diffie-Hellman

Its definition

Let P be a prime and G a primitive root (or generator) of the group

$$\mathbb{Z}_P^* = \{G^0 = 1 = G^{P-1}, G^1 = G, G^2, G^3, \ldots, G^{P-2}\}$$

Definition (Diffie-Hellman)

Let two parties choose positive secret numbers $1 < x, y < P - 1$
and publish $X = G^x \pmod{P}$ and $Y = G^y \pmod{P}$.
The two parties now have a shared secret: $G^{xy} \pmod{P}$.
X knows

$$G^{xy} \equiv (G^y)^x \equiv Y^x \pmod{P}$$

Y knows

$$G^{xy} \equiv (G^x)^y \equiv X^y \pmod{P}$$

Note that nobody knows xy.

Difficult problems

Definition (The factorisation problem)

The integer factorisation problem, that is to reconstruct p and q from $N = pq$, is supposed to be a hard problem.

Definition (DLP or discrete logarithm problem)

The discrete logarithm problem, that is to reconstruct x from $X = G^x \pmod{P}$, is supposed to be a hard problem.

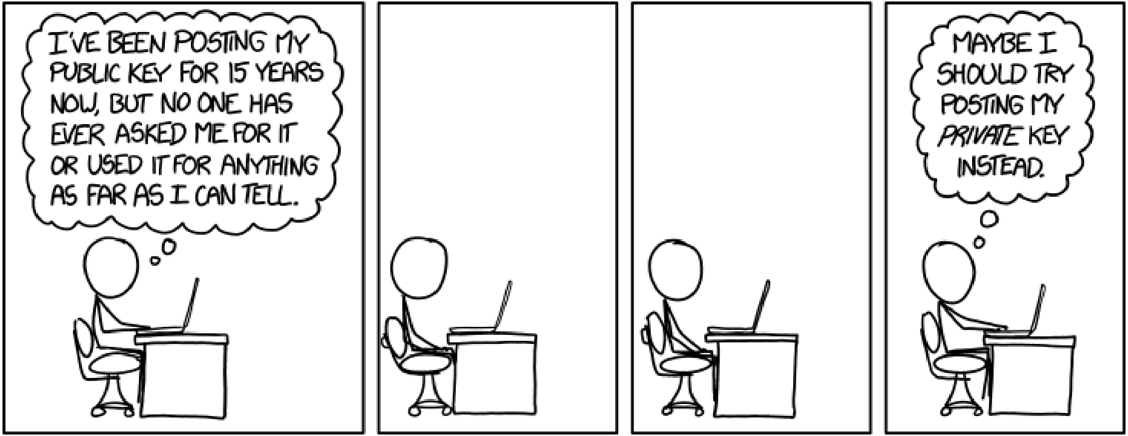
WARNING

Once quantum computers become a reality, these problems become easy to solve.

Part II

More advanced math

All this complexity, for what...?



Source: `https://xkcd.com/1553/`

Outline

Outline

The ring of polynomials over a field

Definition

$\mathbb{F}[X] = \{a_nX^n + \cdots + a_1X + a_0 \mid n \in \mathbb{N}, \text{all } a_i \in \mathbb{F}, a_n \neq 0 \text{ if } n > 0\}$
is the ring[a] of (formal) polynomials in the variable X.
The degree of $f \in \mathbb{F}[X]$ is the highest exponent n of X.

[a] A ring is like a field, but possibly without multiplicative inverses

Theorem (Euclidean division of polynomials)

- *In $\mathbb{F}[X]$ one can add and multiply polynomials as usual.*
- *In $\mathbb{F}[X]$ the equivalent of Euclid's algorithm works.*
    - *For any $f \in \mathbb{F}[X]$ and $g \in \mathbb{F}[X]$ with $g \neq 0$ there are $q \in \mathbb{F}[X]$ and $r \in \mathbb{F}[X]$ such that $f = qg + r$ where r has lower degree than g.*
    - *We write $f \equiv r \pmod{g}$*

Examples of polynomial arithmetic

Examples (Addition and multiplication)

$(X^2 - 3X + 4) + (X^3 - X^2 + 2X - 6) = X^3 - X - 2$
$(X^2 - 3X + 4) \cdot (X^3 - X^2 + 2X - 6) = X^5 - 4X^4 + 9X^3 - 16X^2 + 26X - 24$

Examples (Reduction modulo the polynomial $X^2 + X + 1$)

$$\begin{aligned} X^3 + 3X - 4 &= X(X^2 + X + 1) - X^2 + 2X - 4 \\ &= X(X^2 + X + 1) - 1(X^2 + X + 1) + 3X - 3 \\ &= (X - 1)(X^2 + X + 1) + 3X - 3 \end{aligned}$$

So $X^3 + 3X - 4 \equiv 3X - 3 \pmod{X^2 + X + 1}$

The equivalents of the primes in $\mathbb{F}[X]$

Definition

A polynomial g is called irreducible in $\mathbb{F}[X]$ if there are no lower degree polynomials h and k, both of degree at least 1, such that $g = hk$.

Theorem

If g is irreducible then

$$\mathbb{F}[X]/(g) = \{f \pmod{g} \mid f \in \mathbb{F}[X]\}$$

is a field.

Examples of irreducible polynomials

Examples (using $\mathbb{R}$ and $\mathbb{C}$)

- $X^2 + 1$ is irreducible in $\mathbb{R}[X]$ and $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$
- $X^2 + 1$ is reducible in $\mathbb{C}[X]$
- $X^2 - \frac{7}{6}X + \frac{1}{3}$ is reducible in $\mathbb{Q}[X]$

Examples (Algebraic Number Fields, using $\mathbb{Q}$)

- $X^2 - 2$ is irreducible in $\mathbb{Q}[X]$ and $\mathbb{Q}[X]/(X^2 - 2) \cong \mathbb{Q}(\sqrt{2})$
- $X^2 + X + 1$ is irreducible in $\mathbb{Q}[X]$ and $\mathbb{Q}[X]/(X^2 + X + 1) \cong \mathbb{Q}(-1/2 + 1/2i\sqrt{3})$

Outline

More examples of polynomial arithmetic

Examples (Addition and multiplication with coefficients in $\mathbb{Z}_2$)

$(X^2 + X + 1) + (X^2 + 1) = X$
$(X^2 + X + 1) \cdot (X^2 + 1) = X^4 + X^3 + X + 1$
$(f + g)^2 = f^2 + g^2$ ("Freshman's dream")

Examples (Addition and multiplication with coefficients in $\mathbb{Z}_3$)

$(X^2 + X + 1) + (X^2 + 1) = 2X^2 + X + 2 = -X^2 + X - 1$
$(X^2 + X + 1) \cdot (X^2 + 1) = X^4 + X^3 + 2X^2 + X + 1 = X^4 + X^3 - X^2 + X + 1$
$(f + g)^2 = f^2 + g^2 - f \cdot g$ ("“Freshman's nightmare”")

Examples of (ir)reducible polynomials

Examples

- $X^2 + 1$ is not irreducible over $\mathbb{Z}_2$,
  for we have $X^2 + 1 = X^2 + 2X + 1 = (X + 1)^2$
- $X^2 + X + 1$ is irreducible over $\mathbb{Z}_2$
- $X^2 + X + 1$ is not irreducible over $\mathbb{Z}_3$,
  for we have $X^2 + X + 1 = X^2 + 4X + 4 = (X + 2)^2$
- $X^2 + 1$ is irreducible over $\mathbb{Z}_3$
- $X^2 + 2X + 2$ is also irreducible over $\mathbb{Z}_3$

Outline

Outline

Irreducibles over $\mathbb{Z}_p$

Theorem

- *Taking $\mathbb{F} = \mathbb{Z}_p$ for a prime p and g an irreducible polynomial of degree n, with coefficients in $\mathbb{F}$, $\mathbb{F}[X]/(g)$ is a field with p^n elements.*
- *For any prime p and natural number $n > 0$ there is exactly one field, denoted $GF(p^n)$ or $\mathbb{F}_{p^n}$, with p^n elements (up to isomorphism).*

In honour of Évariste Galois these finite fields are also called Galois fields.
Uniqueness up to isomorphism tells you it doesn't matter
which irreducible polynomial is used for the construction.

Properties of finite fields

and their cyclic multiplicative subgroups

Theorem

For any finite field $\mathbb{F}$

- $|\mathbb{F}| = p^n$, *where* p *is a prime called the characteristic of* $\mathbb{F}$, *being the smallest number for which the* p*-time repetition* $1 + 1 + \ldots + 1$ *is equal to* 0.
- *The multiplicative group of* $\mathbb{F}$ *is always cyclic.*
- *The irreducible polynomial* g *is called* *primitive* *if* X *is a generator of this (cyclic) multiplicative group.*
- $GF(p) \cong \mathbb{Z}_p$, *but beware:*
  - *For* $n > 1$: $GF(p^n) \ncong (\mathbb{Z}_p)^n$
  - *For* $n > 1$: $GF(p^n) \ncong \mathbb{Z}_{p^n}$

Examples of finite fields and primitive polynomials

Examples

- $X^2 + X + 1$ is (irreducible and) primitive over $GF(2)$.
- $GF(4) = GF(2^2) = \mathbb{Z}_2[X]/(X^2 + X + 1) =$
  $\{0\} \cup \{X, X^2 = X + 1, X^3 = X^2 + X = X + 1 + X = 1\}$ with generator X.
- $X^2 + 1$ is irreducible, but not primitive over $GF(3)$.
- $X^2 + 2X + 2$ is (irreducible and) primitive over $GF(3)$.
- $GF(9) = GF(3^2) = \mathbb{Z}_3[X]/(X^2 + 2X + 2) =$
  $\{0\} \cup \{X, X^2 = X + 1, X^3 = 2X + 1, X^4 = 2, X^5 = 2X, X^6 = 2X + 2, X^7 = X + 2, X^8 = 1\}$

Outline

Use of Galois Fields in AES

- The *S-box* uses polynomials over $GF(2)$
  - The inverse modulo the irreducible $x^8 + x^4 + x^3 + x + 1$
  - Multiplication by $x^4 + x^3 + x^2 + x + 1$ modulo the (reducible) $x^8 + 1$
  - Addition of $x^6 + x^5 + x + 1$ also modulo the (reducible) $x^8 + 1$
- *MixColumn* uses polynomials with coefficients over $GF(2^8)$ modulo the reducible polynomial $x^4 + \mathbf{01}$
  - $GF(2^8) \cong \mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x + 1)$, represented by hex digits **XY**
  - Multiplication by $\mathbf{03}x^3 + \mathbf{01}x^2 + \mathbf{01}x + \mathbf{02}$
    and for the inverse by $\mathbf{0B}x^3 + \mathbf{0D}x^2 + \mathbf{09}x + \mathbf{0E}$
- *Key expansion* uses
  - Arithmetic in $GF(2^8)$ for generating the constants $C_i = x^i$
    working modulo the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$
  - The polynomial x^3 modulo $x^4 + \mathbf{01}$ over $GF(2^8)$
    for rotations of columns

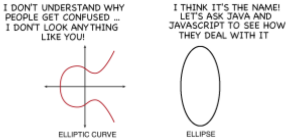
For a concise treatment of Rijndael (AES) for algebraists by Hendrik Lenstra, see

`http://www.math.berkeley.edu/~hwl/papers/rijndael0.pdf`

Part III

Advanced math

Ellipses? No!



Source: `https://prateekvjoshi.com/2015/02/07/why-are-they-called-elliptic-curves/`

Outline

Mathematical background

needed to really understand Elliptic Curves

- Advanced Algebra
  - Algebraic Geometry
  - Algebraic Number Theory
  - Galois Theory
- Deep relations...
  - ...with lattices
  - ...with modular forms
  - ...with Fermat's Last Theorem
- "You are not expected to understand this."[1]

[1] https://en.wikipedia.org/wiki/Lions'_Commentary_on_UNIX_6th_Edition,_with_Source_Code

Outline

6. Elliptic Curves
   - A strange group
   - Some applications in cryptography
   - An option for a backdoor?

Definition of an elliptic curve

in a simplified case

Definition

An elliptic curve consists of the solutions (x, y) of a cubic equation $y^2 = x^3 + ax + b$, where a, b, x and y are elements of a field. For our case we demand the field to be a finite one ($\mathbb{F}_q$), with $q = p^n$, in most cases $n = 1$ and $p > 3$.
We also demand that $4a^3 + 27b^2 \neq 0$, which means there are no singularities.
Finally we add one extra point "at infinity".

Example

Consider the curve $y^2 = x^3 + 2x + 1$ over $\mathbb{F}_5$.
This is an elliptic curve with 6 finite points on it:
(0,1) (0,4), (1,2), (1,3), (3,2), (3,3).
There is also the special (7^{th}) point at infinity...,
which will work as 0 for addition, to be defined.

Addition on an elliptic curve

Definition (Point at infinity)

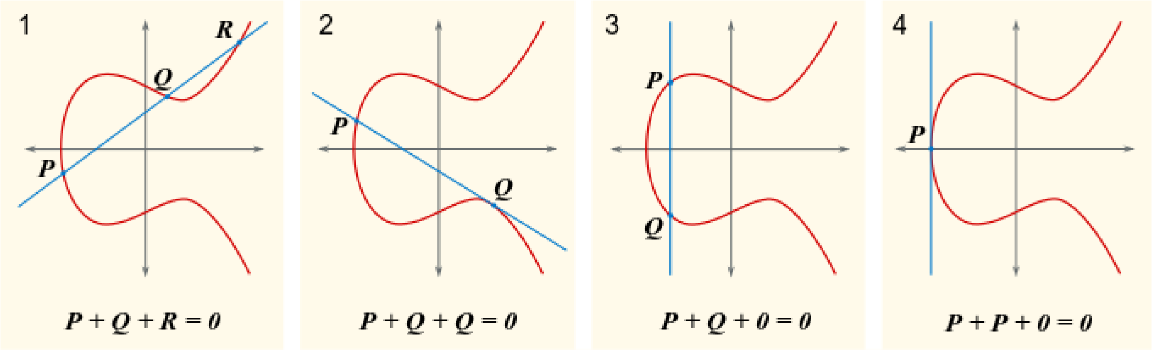
By adding a point at infinity to every elliptic curve we work in projective space, which moreover enables an operation of addition to be defined, turning the curve into an abelian group.

Theorem

On an elliptic curve an addition can be defined with the property that if a straight line intersects the curve in three points P, Q and R the relation $P + Q + R = 0$ holds. This addition turns the elliptic curve into an abelian group with 0 (the point at infinity) as the neutral element.

Notation: $[n]P = P + \ldots + P$, with P repeated n times.

Geometric intuition



Source: `https://commons.wikimedia.org/wiki/File:ECClines.png`

Outline

Structure of an EC group

Theorem (Structure of an elliptic curve group)

Every elliptic curve group $\mathbb{E}(\mathbb{F}_q)$ where $q = p^n$ and $p > 3$ is of the form

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

where $n_2 \mid n_1$ and $n_2 \mid q - 1$.

One can find an elliptic curve over $\mathbb{F}_p$ such that its group is cyclic with order some prime $g \neq p$.
This curve[2] can be used for a Diffie-Hellman construction.

[2] If we have $g = p$ the curve is anomalous and not secure

Diffie-Hellman over an elliptic curve

The simplest case

Let $\mathbb{E}$ be an elliptic curve over $\mathbb{F}_p$ with a cyclic additive group of prime order $g \neq p$ and let the point G on $\mathbb{E}$ be a generator of this group.
So $E = \{G, [2]G, [3]G, \ldots, [g-1]G, [g]G = 0\}$.

Definition (ECDH, Elliptic Curve Diffie-Hellman)

Let two parties A and B choose secret numbers $1 < a, b < g$ and publish $P = [a]G$ and $Q = [b]G$. Only A knows a and only B knows b.
The two parties now have a shared secret: $[ab]G$.
A knows

$$[a](Q) = [a]([b]G) = [ab]G$$

B knows

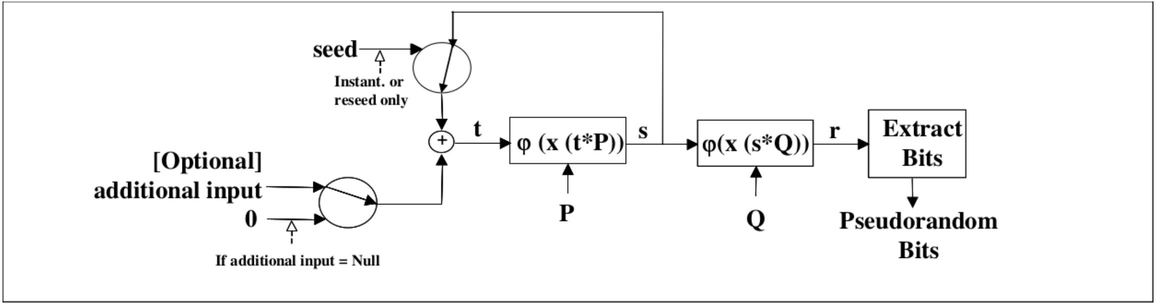
$$[b](P) = [b]([a]G) = [ba]G = [ab]G$$

Other observers, without knowledge of a or b, are confronted with the (supposedly) difficult ECDLP of calculating a and/or b from P and/or Q.

Outline

6 Elliptic Curves
- A strange group
- Some applications in cryptography
- An option for a backdoor?

The original NIST Dual EC DRBG algorithm



Source: NIST SP 800-90A

General scheme for typical PRNGs

$$
\begin{tikzcd}
\text{secret state} & S_0 \arrow[r, "f"] \arrow[d, "g"] & S_1 \arrow[r, "f"] \arrow[d, "g"] & S_2 \arrow[r, "f"] \arrow[d, "g"] & S_3 \arrow[r, "f"] \arrow[d, "g"] & S_4 \arrow[r, "f"] \arrow[d, "g"] & \cdots \\
\text{random bits} & R_0 & R_1 & R_2 & R_3 & R_4 &
\end{tikzcd}
$$

Backdoored PRNG

$$\begin{tikzcd}
S_0 \arrow[r, "f"] \arrow[d, "g"] & S_1 \arrow[r, "f"] \arrow[d, "g"] & S_2 \arrow[r, "f"] \arrow[d, "g"] & S_3 \arrow[r, "f"] \arrow[d, "g"] & S_4 \arrow[r, "f"] \arrow[d, "g"] & {} & \cdots \\
R_0 \arrow[ur, dashed] & R_1 \arrow[ur, dashed] & R_2 \arrow[ur, dashed] & R_3 \arrow[ur, dashed] & R_4 \arrow[ur, dashed] & &
\end{tikzcd}$$

Surreptitious Diffie-Hellman

$$\begin{tikzcd} s \arrow[r, "*P"] \arrow[d, "*Q"'] & s' \\ r \arrow[ur, dashed] & \end{tikzcd}$$

$$\begin{tikzcd} Q \arrow[r, "{[?]}"] \arrow[d, "{[s]}"'] & P \arrow[d, "{[s]}"] \\ R \arrow[r, dashed, "{[?]}"] & S' \end{tikzcd}$$

$*P$ is shorthand for $\phi(x(. * P))$

Effect on elliptic curve points

Spoiled surreptitious Diffie-Hellman

$$
\begin{tikzcd}
s \arrow[r, "h"] \arrow[d, "*Q"'] & \cdot \arrow[r, "*P"] & s' \arrow[r, "h"] \arrow[d, "*Q"'] & \cdot \arrow[r, "*P"] & s'' \arrow[d, "*Q"'] \\
r \arrow[ur, dashed, "?"'] & & r' & & r''
\end{tikzcd}
$$

The trick is spoiled by the presence of the function h,
which xors in some hash of the additional input.

Repaired surreptitious Diffie-Hellman

$$\begin{tikzcd}
s \arrow[r, "h"] & \cdot \arrow[r, "*P"] & \cdot \arrow[r, "*P"] \arrow[d, "*Q"'] & s' \arrow[r, "h"] & \cdot \arrow[r, "*P"] & \cdot \arrow[r, "*P"] \arrow[d, "*Q"'] & s'' \\
 & & r \arrow[ur, dashed, "!"'] & & & r' &
\end{tikzcd}$$

The trick is back because of the extra *P operation,
introduced without adapting the picture in the 2007 version of the specification.

The NIST Dual EC DRBG backdoor option

$$
\begin{tikzcd}
 & s \arrow[r] & {[s]P} \arrow[d, "\text{x coordinate}"] & \\
{[t]P} \arrow[d, "\text{x coordinate}"] & & t \arrow[ll] \arrow[r] & {[t]Q} \arrow[d, "\text{bits from x coordinate}"'] \\
s' & & & r
\end{tikzcd}
$$

Now suppose "someone" knows the secret relation $P = [?]Q$.
Then a surreptitious DH exchange can be performed when r is used.
First find the few possibilities for [t]Q from r. Then

$$[t]P = [t][?]Q = [t?]Q = [?t]Q = [?][t]Q$$