Literature recommendation.

JK Rowling: Harry Potter and the Philosopher's Stone

F Dostoevsky: Crime and Punishment.

JRR Tolkien: The Lord of the Rings.

Cormen, Leiserson, Rivest, Stein:
Introduction to Algorithms, Fourth Edition
Chapter 31: elementary introduction into $\mathbb{Z}_n$ and the RSA

German Edition: Algorithmen – eine Einführung

Theorem 5 (Bézout's Identity) For every choice of $a, b \in \mathbb{Z}$ there exists numbers $s, t \in \mathbb{Z}$ such that

$$s \cdot a + t \cdot b = \gcd(a, b)$$

Proof: Since we analyzed EA and EEA and we know, why the work (they terminate giving correct results), the assertion is a byproduct of this analysis. □

Quick example: $(-2) \cdot 3 + 1 \cdot 7 = 1$

What is the running time of EA, EEA?
We estimate the number of iterations.

Example. Let's do gcd calculations in the binary system.

$a = 13$

$b = 21$ (in decimal)

$a = 1101$

$b = 10101$ (in binary system)

$\gcd(1101, 10101) = \gcd(1101, 10101 - 1101)$ (1101: 4 binary digits)

$= \gcd(1101, 1000)$

$= \gcd(1000, 1101)$ (1000: still 4 binary digits)

$= \gcd(1000, 1101 - 1000)$

$= \gcd(1000, 101)$

$= \gcd(101, 1000)$ (101: 3 binary digits)

The digit size of the smaller of the two numbers (in the binary system) is guaranteed to drop within two iterations. So the number of iterations of the EA and EEA is at most twice the number of the binary digits of the smaller number in the input. $\Rightarrow$ The number of iterations is linear in the bit size.

Theorem 6 For $n \in \mathbb{N}$, $n \geq 2$ a coset $[a]$ is invertible in $\mathbb{Z}_n$ if and only if $\gcd(a,n) = 1$.

Proof: If $\gcd(a,n) = 1$, then $s \cdot a + t \cdot n = 1$ for some $s,t \in \mathbb{Z}$ in view of Theorem 5. $\Rightarrow$

$[s] \cdot [a] = [1] \Rightarrow [a]^{-1} = [s]$.

If $\gcd(a,n) = g > 1$, then $\left[\frac{n}{g}\right] \neq [0]$ and

$[a] \cdot \left[\frac{n}{g}\right] = \left[a \cdot \frac{n}{g}\right] = \left[\left(\frac{a}{g}\right) \cdot n\right] = [0]$. So when $[a] \neq [0]$,

$\frac{a}{g} \in \mathbb{Z}$

if a zero divisor and thus not invertible. (if $[a]=[0]$, then it's zero and not invertible anyway. □

Example $\mathbb{Z}_{15}$

[6] $\gcd(6,15)=3$

$$[6]\cdot[5] = [6]\cdot\left[\tfrac{15}{3}\right] = \left[\tfrac{6}{3}\cdot 15\right] = [2\cdot 15] = [0]!$$

$\Rightarrow$ [6] is zero divisor and by this not invertible.

[8] $\gcd(8,15)=1$ $\xrightarrow{\text{EEA}}$ $2\cdot 8 + (-1)15 = 1$

$$[2]\cdot[8] = [2\cdot 8] = [1-(-1)\cdot 15] = [1] \Rightarrow$$

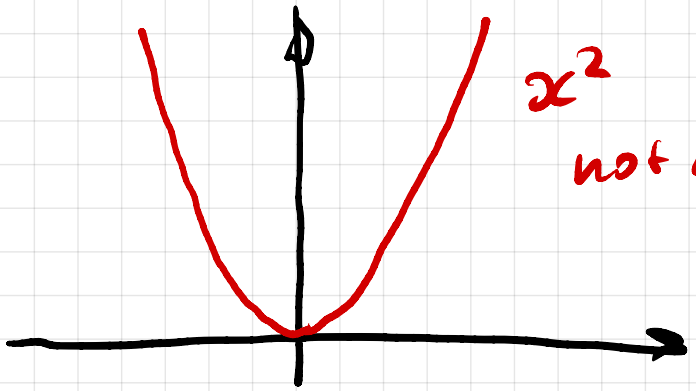
$$[8]^{-1} = [2].$$

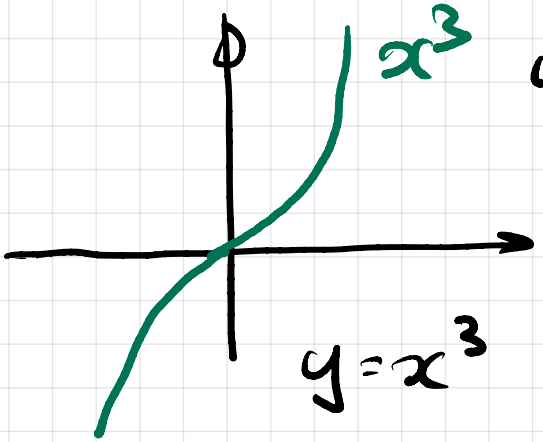
1.3. Little Fermat's theorem and the power functions

Functions like $f(x) = ax + b$ on $\mathbb{Z}_n$ are tame/regular etc., not freaky enough for cryptography.

The power functions $f(x) = x^e$ on $\mathbb{Z}_n$ are quite freaky. We want to use them, but for cryptography we need to be able to invert them.

Let's take the field $\mathbb{R}$ of reals for analogy.





x^3 invertible, inverse is also a power function (power $\frac{1}{3}$).

One can do some analysis like this also over $\mathbb{Z}_n$.

Theorem 7 (Little Fermat's Theorem). Let p be a prime number. Then $a^{p-1} = 1$ for every $a \in \mathbb{Z}_p \setminus \{0\}$.

Proof: Remember that $\mathbb{Z}_p$ is a field (see Theorem 3). Hence, $a \cdot x \neq 0$ for every $x \in \mathbb{Z}_p \setminus \{0\}$. So, we can define a function $f: \mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}_p \setminus \{0\}$ by $f(x) = a \cdot x$. Since $a \neq 0$, f is a bijective linear function. $\Rightarrow$ When we let x go over all non-zero elements of $\mathbb{Z}_p$ exactly once, $a \cdot x$ goes over all non-zero elements of $\mathbb{Z}_p$ exactly once, too, but in some other order. $\Rightarrow$

$$\prod_{x \in \mathbb{Z}_p \setminus \{0\}} x = \prod_{x \in \mathbb{Z}_p \setminus \{0\}} (a \cdot x)$$

$$\Rightarrow \prod_{x \in \mathbb{Z}_p \setminus \{0\}} x = a^{p-1} \cdot \prod_{x \in \mathbb{Z}_p \setminus \{0\}} x$$

The same product, which is non-zero because it is a product of non-zero elements.

Dividing the equation by this product we obtain $1 = a^{p-1}$. □

Rem Let's clasify why $f(x) = ax$ with $a \neq 0$, $f: \mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}_p \setminus \{0\}$ is bijective. For this, it suffices to check that $g(x) = \bar{a}^1 \cdot x$ is the inverse of f.

$$g(f(x)) = f(g(x))$$

$$\| \qquad\qquad \|$$

$$\bar{a}^1 \cdot a \cdot x \qquad a \cdot \bar{a}^1 \cdot x$$

$$\| \qquad\qquad \|$$

$$x \qquad\qquad x$$

$$f(x') = f(x'') \Rightarrow g(f(x')) = g(f(x''))$$

$$\Rightarrow x' = x'' \quad \text{(injectivity)}.$$

If you want to realize $y \in \mathbb{Z}_p \setminus \{0\}$ as an output for some input, you clearly do this: $x = g(y) = a^{-1} \cdot y$

$$\Rightarrow f(x) = a \cdot x = a \cdot a^{-1} \cdot y = y.$$

Rem There are several slightly different formulations of this theorem.

- $a^p = a$ for every $a \in \mathbb{Z}_p$.
- If you take $a = [z]$ with $z \in \mathbb{Z}$, you can also say that $z^{p-1} \equiv 1 \pmod{p}$ whenever z is not divisible by p.
- $z^p \equiv z \pmod{p}$ for every $z \in \mathbb{Z}$.

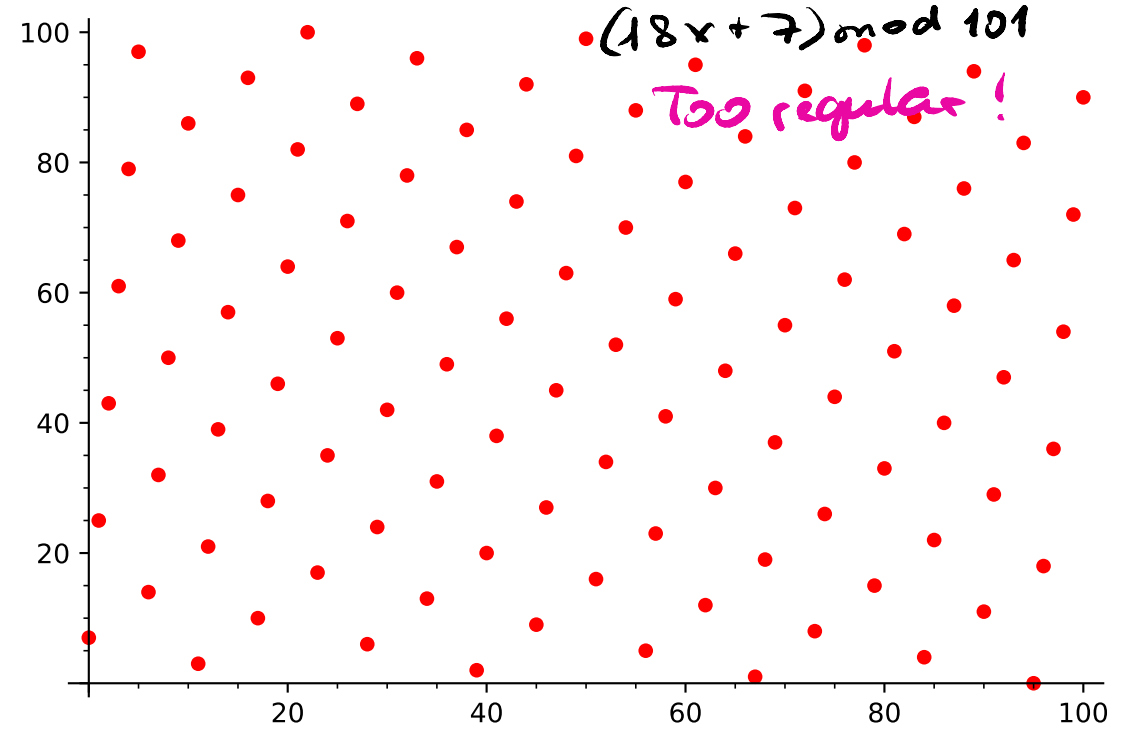
Example

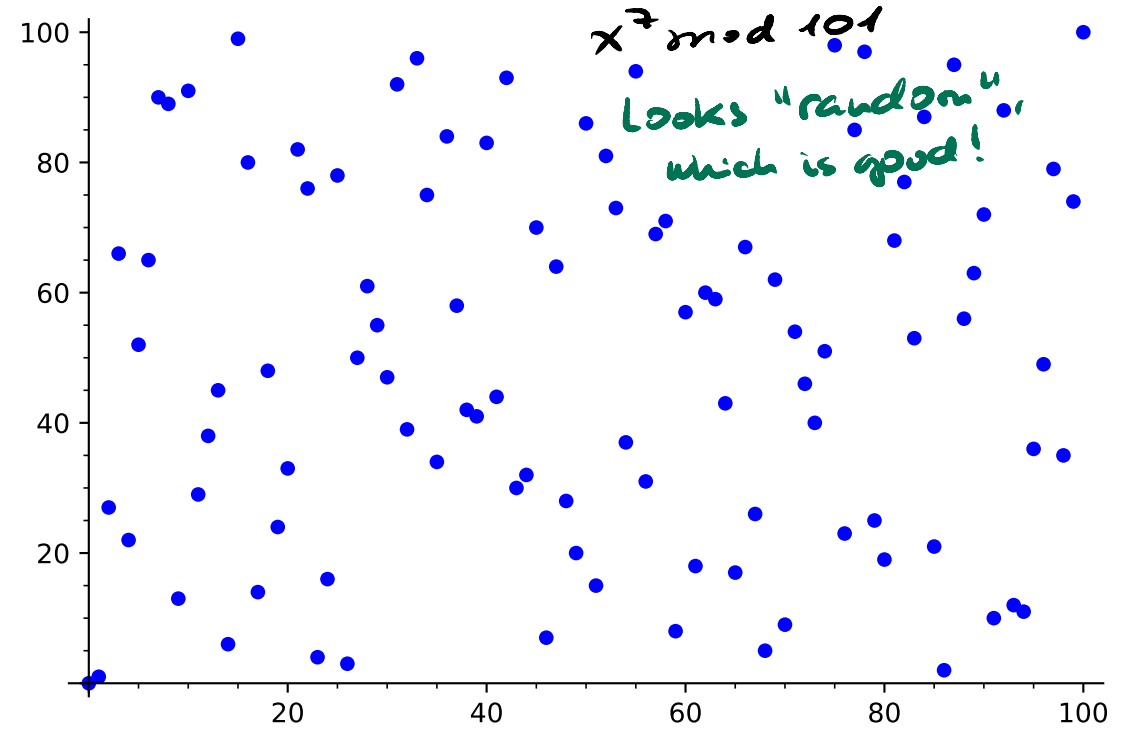
$a = [2]$ in $\mathbb{Z}_7$

x	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$a \cdot x$	$[2]$	$[4]$	$[6]$	$[1]$	$[3]$	$[5]$

$$[1] \cdot [2] \cdot [3] \cdot [4] \cdot [5] \cdot [6] = (a \cdot [1]) \cdot (a \cdot [2]) \cdot (a \cdot [3]) \cdot (a \cdot [4]) \cdot (a \cdot [5]) \cdot (a \cdot [6])$$

$$\Rightarrow \quad 1 = a^6 .$$


(18x+7) mod 101
Too regular!
100
80
60
40
20
20
40
60
80
100


$x^7 \bmod 101$
Looks "random",
which is good!
100
80
60
40
20
20
40
60
80
100

Remark We have a collection of power functions $f(x) = x^e$ on $\mathbb{Z}_p$, and we want to see which ones we could deploy for decryption.

$p = 11$ as an example:

$x^1, x^2, x^3, x^4, x^5, x^6, x^7, x^8, x^9, x^{10}, x^{11}, x^{12}, \ldots, x^{21}$

$x^{11} = x^1 \quad x^{12} = x^2$

If we work with the base modulo p, we can work with the exponents modulo $p-1$.

In particular, $x^1, \ldots, x^{p-1}$ are all possible power functions. Some of these functions are bijective (& good for cryptography) and some not (not good for cryptography).

x^1 invertible ; the inverse is x^1 : $(x^1)^1 = x$

x^2 not invertible; $1^2 = (-1)^2 = 1$

$$1 = [1]$$
$$-1 = [10]$$

x^3 is invertible ; the inverse is x^7

$$(x^3)^7 = (x^7)^3 = x^{21} = x^1 \cdot (x^{10})^2 = x^1 = x$$

by Theorem 7.

x^5 not invertible ; the reason $\gcd(5, 10) \neq 1$.

"p-1.

x^9 is invertible and the inverse x^9

$$(x^9)^9 = x^{81} = (x^{10})^8 \cdot x = x.$$

Corollary 8 Let p be prime. Let $e \in \mathbb{N}$ be a number with $\gcd(e, p-1) = 1$. Then there exists $d \in \{1, \dots, p-1\}$ such that x^d is the inverse function of x^e on $\mathbb{Z}_p$.

That means $(x^e)^d = (x^d)^e = x$ for every $x \in \mathbb{Z}_p$.

Proof: By Theorem 6, $[e]_{p-1}$ is invertible in $\mathbb{Z}_{p-1}$.

Thus, there exists $[d]_{p-1}$ with $d \in \{1, \dots, p-1\}$ such that

$[e]_{p-1} \cdot [d]_{p-1} = [1]_{p-1}$ (you can find d via EEA).

But that means $e \cdot d = 1 + k \cdot (p-1)$ for some non-negative integer k. $\Rightarrow$

$$(x^e)^d = (x^d)^e = x^{ed} = x^{1 + k \cdot (p-1)}$$

$$= x \cdot (x^{p-1})^k \underset{\text{by theorem 7.}}{=} x.$$

□

Goodnotes advice from Sol:

Zoom in tool

Voice recording

Goodnotes → GitHub.

Testing within the lectures

Calculators?