Cryptography (and Information Security) 6CCS3CIS / 7CCSMCIS

Prof. Luca Viganò

Department of Informatics
King's College London, UK

First term 2020/21

Lecture 7.1: Some number theory

Table of contents I

Table of contents I

Prime factorization

- Numbers: **naturals** $\mathbb{N} = \{0, 1, 2, \ldots\}$, **integers** $\mathbb{Z} = \{0, 1, -1, \ldots\}$, **primes** $\mathcal{P} = \{2, 3, 5, 7, ...\}$.
- To **factor** a number a is to write it as a product of other numbers, e.g., $a = b \times c \times d$.
- Multiplying numbers is easy, factoring numbers appears hard. We cannot factor most numbers with more than 1024 bits.
- The **prime factorization** of a number a amounts to writing it as a product of powers of primes:

$$a = \prod_{p \in \mathcal{P}} p^{a_p} = 2^{a_2} \times 3^{a_3} \times 5^{a_5} \times 7^{a_7} \times 11^{a_{11}} \times \ldots \quad \text{where } a_p \in \mathbb{N}$$

  For any particular value of a, most of the exponents a_p will be 0, e.g.,

$$\begin{aligned} 91 &= 7 \times 13 \\ 3600 &= 2^4 \times 3^2 \times 5^2 \\ 11011 &= 7 \times 11^2 \times 13 \end{aligned}$$

Divisors

$a \neq 0$ **divides** b (written $a \mid b$) if there is an m such that $m \times a = b$.

- Examples: $3 \mid 6$ and $7 \mid 21$.

a **does not divide** b (written $a \nmid b$) if there is no m such that $m \times a = b$.

- Examples: $3 \nmid 7$, $3 \nmid 10$ and $7 \nmid 22$.

Relatively prime numbers & greatest common divisor

Two natural numbers a, b are **relatively prime** if they have no common divisors/factors apart from 1, i.e., if their **greatest common divisor** gcd is equal to 1

$$\gcd(a,b) = 1 \,.$$

- For example, 8 and 15 are relatively prime since
  - factors of 8 are 1, 2, 4, 8,
  - factors of 15 are 1, 3, 5, 15,
  - and 1 is the only common factor.
- Conversely, we can determine the greatest common divisor by comparing their prime factorizations and using least powers, e.g.
  - $150 = 2^1 \times 3^1 \times 5^2$ and $18 = 2^1 \times 3^2$, thus $\gcd(18, 150) = 2^1 \times 3^1 \times 5^0 = 6$.
  - $60 = 2^2 \times 3 \times 5$ and $14 = 2 \times 7$, thus $\gcd(60, 14) = 2$.

Table of contents I

Greatest common divisor and Euclid's algorithm

- gcd can be computed quickly using **Euclid's algorithm**.

$$\begin{array}{llcl} \gcd(60,14) & : & 60 & = & (4 \times 14) + 4 \\ \gcd(14,4) & : & 14 & = & (3 \times 4) + 2 \\ \gcd(4,2) & : & 4 & = & 2 \times 2 \end{array}$$

- **Extended Euclid's algorithm** computes $x, y \in \mathbb{Z}$ such that

$$\gcd(a,b) = (x \times a) + (y \times b)$$

Here $2 = 14 - 3 \times (60 - (4 \times 14)) = (-3 \times 60) + (13 \times 14)$

Euclid's Algorithm

Euclid's algorithm is based on the theorem

$\gcd(a, b) = \gcd(b, a \bmod b)$ for any nonnegative integer a and any positive integer b.

For example:

- $\gcd(55, 22) = \gcd(22, 55 \bmod 22) = \gcd(22, 11) = 11$.

Euclid's algorithm

Euclid(a, b)
1 **if** $b = 0$
2 **then return** a
3 **else return** Euclid$(b,\ a \bmod b)$

For example:

- Euclid$(30, 21)$ = Euclid$(21, 9)$ = Euclid$(9, 3)$ = Euclid$(3, 0)$ = 3.

Extended Euclid's Algorithm

Extend Euclid's algorithm to compute integer coefficients x, y such that

$$d = \gcd(a, b) = (a \times x) + (b \times y)$$

Extended Euclid's algorithm

```
Extended-Euclid(a, b)
if b = 0
then
    return (a, 1, 0)
else
    (d', x', y') ← Extended-Euclid(b, a mod b)
    (d, x, y) ← (d', y', x' − (⌊a/b⌋ × y'))
    return (d, x, y)
```

where $q = \lfloor a/b \rfloor$ is the **quotient of the division** (for $a = (q \times b) + r$).

Note: the d here is the greatest common **d**ivisor, not to be confused with the d that is (part of) an RSA private key (discussed later on).

Extended Euclid's Algorithm: example

$$\text{Extended-Euclid}(99, 78) = 3 = (99 \times (-11)) + (78 \times 14)$$

```
Extended-Euclid(a, b)
if b = 0
then
    return (a, 1, 0)
else
    (d', x', y') ← Extended-Euclid(b, a mod b)
    (d, x, y) ← (d', y', x' − (⌊a/b⌋ × y'))
    return (d, x, y)
```

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	–	3	1	0

Each line shows one level of the recursion.

Table of contents I

Modular arithmetics

Remainder

- $\forall a\, n.\ \exists q\, r.\ (a = (q \times n) + r)$ where $0 \leq r < n$.
  Here r is the **remainder**, which we write as
  $$r = a \bmod n\,.$$

Congruent modulo

- $a, b \in \mathbb{Z}$ are **congruent modulo** n, if $a \bmod n = b \bmod n$.
  We write this as
  $$a =_n b\,.$$

Modulo operator has following properties (of congruences)

- Reflexivity: $a =_n a$.
- Symmetry: If $a =_n b$ then $b =_n a$.
- Transitivity: If ($a =_n b$ and $b =_n c$) then $a =_n c$.

Other properties of the modulo operator

$(a \bullet b) =_n (a \bmod n) \bullet (b \bmod n) \qquad \text{for } \bullet \in \{+, -, \times\}$

i.e., $(a \bullet b) \bmod n = [(a \bmod n) \bullet (b \bmod n)] \bmod n$

Example:

$$\begin{aligned} 2 &= (5 \times 6) \bmod 4 \\ &= [(5 \bmod 4) \times (6 \bmod 4)] \bmod 4 \\ &= (1 \times 2) \bmod 4 = 2 \bmod 4 = 2 \end{aligned}$$

If $a \times b =_n a \times c$ and a relatively prime to n, then $b =_n c$.

Example:

- $8 \times 4 =_3 8 \times 1$.
- 8 is relatively prime to 3.
- So: $4 =_3 1$.

If $a_1 =_n b_1$ and $a_2 =_n b_2$, then

$$(a_1 + a_2) =_n (b_1 + b_2) \quad \text{and} \quad (a_1 \times a_2) =_n (b_1 \times b_2)$$

- This can also be expressed as

$$[(a_1 \bmod n) + (a_2 \bmod n)] \bmod n = (a_1 + a_2) \bmod n$$

  and

$$[(a_1 \bmod n) \times (a_2 \bmod n)] \bmod n = (a_1 \times a_2) \bmod n$$

- Example: Let $r_a = a \bmod n$ and $r_b = b \bmod n$.
  Then, there are integers j and k such that

$$a = r_a + jn \text{ and } b = r_b + kn$$

  and we can proceed as follows:

$$\begin{aligned}
(a+b) \bmod n &= (r_a + jn + r_b + kn) \bmod n \\
&= (r_a + r_b + (j+k)n) \bmod n \\
&= (r_a + r_b) \bmod n \\
&= [(a \bmod n) + (b \bmod n)] \bmod n
\end{aligned}$$

- $a = q \times n + r$ with $q = \lfloor a/n \rfloor$ and $0 \leq r < n$ and $r = a \bmod n$
- For any integer a, we can rewrite this as follows:
  $a = \lfloor a/n \rfloor \times n + (a \bmod n)$

Then, for example:

- $11 \bmod 7 = 4$
- $-11 \bmod 7 = -4$ ($= 3$ when reasoning modulo 7)
- $73 =_{23} 4$
- $21 =_{10} -9$
- $147 =_{220} -73$

- If $a =_n 0$ then $n \mid a$
- $a =_n b$ if $n \mid (a - b)$

- To demonstrate the last point, if $n \mid (a - b)$, then $(a - b) = k \times n$ for some k.

  So we can write $a = b + (k \times n)$.

  Therefore, (a mod n) = (remainder when $b + (k \times n)$ is divided by n) = (remainder when b is divided by n) = (b mod n).
- Then, for example:
  - $23 =_5 8$ because $23 - 8 = 15 = 5 \times 3$
  - $-11 =_8 5$ because $-11 - 5 = -16 = 8 \times (-2)$
  - $81 =_{27} 0$ because $81 - 0 = 81 = 27 \times 3$

Modular arithmetics: two theorems

Theorem

Suppose that $a, b \in \mathbb{Z}$ are relatively prime. There is a $c \in \mathbb{Z}$ satisfying $(b \times c) \bmod a = 1$, i.e., we can compute $b^{-1} \bmod a$.

Proof: From the Extended Euclid's Algorithm, there exist $x, y \in \mathbb{Z}$ where

$$1 = (a \times x) + (b \times y)$$

Since $a \mid (a \times x)$, we have $(b \times y) \bmod a = 1$.
Assertion follows with $c = y$.

Fermat's little theorem

For a and n relatively prime and n prime

$$a^{n-1} =_n 1$$

Example: $4^6 \bmod 7 = (16 \times 16 \times 16) \bmod 7 = (2 \times 2 \times 2) \bmod 7 = 1$.

Proof of Fermat's Little Theorem

- Consider the set $\{1, 2, \ldots, n-1\}$ of positive integers less than n.
- Multiply each element by a, modulo n, to get the set $X = \{a \bmod n, 2a \bmod n, \ldots, (n-1)a \bmod n\}$.
- We can prove that:
  - None of the elements of X is equal to 0 because n does not divide a.
  - Furthermore, no two of the integers in X are equal.
    - To see this, assume that $x \times a =_n y \times a$ for $1 \leq x < y \leq n-1$.
    - Because a and n are relatively prime, we can eliminate a from both sides and obtain $x =_n y$, which is impossible as we assumed that x and y are both positive integers less than n, with $x < y$.
- Therefore, we know that the $(n-1)$ elements of X are all positive integers with no two elements equal.
- Hence, X consists of the set of integers $\{1, 2, \ldots, n-1\}$ in some order.
- Multiplying the numbers in both sets, and taking the result $\bmod n$ yields

$$
\begin{aligned}
a \times 2a \times \ldots \times (n-1)a &=_n [1 \times 2 \times \ldots \times (n-1)] \\
a^{n-1} \times (n-1)! &=_n (n-1)!
\end{aligned}
$$

- As n is prime, $(n-1)!$ is relatively prime to n; so canceling the $(n-1)!$ yields

$$a^{n-1} =_n 1$$

Table of contents I

Euler Totient Function

- When doing arithmetic modulo n.
- Complete set of **residues** is $0, \ldots, n-1$.
- **Reduced set of residues** consists of those numbers (*residues*) that are relatively prime to n.

  For instance, for $n = 10$:
  - complete set of residues is $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$,
  - reduced set of residues is $\{1, 3, 7, 9\}$.
- Number of elements in reduced set of residues is called the **Euler Totient Function** $\phi(n)$.
  - In other words, $\phi(n)$ **is the number of positive integers less than** n **which are relatively prime to** n, i.e.,
    $\phi(n)$ is the number of $a \in \{1, 2, \ldots, n-1\}$ with $\gcd(a, n) = 1$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Euler's Totient Function and Euler's Theorem

Properties:

- $\phi(1) = 1$.
- $\phi(p) = p - 1$ if p is prime.
- $\phi(p \times q) = \phi(p) \times \phi(q) = (p - 1) \times (q - 1)$ if p and q are prime and $p \neq q$.

So that Fermat's little theorem (for a and n relatively prime and n prime) can be rewritten to

Euler's Theorem

$a^{\phi(n)} =_n 1$ for all a, n such that n is prime and $\gcd(a, n) = 1$.

Examples:

- If $a = 3$ and $n = 10$, then $\phi(10) = 4$ and $3^4 = 81 =_{10} 1$
- If $a = 2$ and $n = 11$, then $\phi(11) = 10$ and $2^{10} = 1024 =_{11} 1$

Bibliography

- William Stallings. *Cryptography and Network Security. Principles and Practice*, 7th ed., Prentice Hall, 2016.
- Keith Martin. *Everyday Cryptography*, 2nd ed., Oxford, 2017.
- Dieter Gollmann. *Computer Security*. Wiley, 2011.
- Bruce Schneier. *Applied Cryptography*, John Wiley & Sons, 1996 (and 20th anniversary edition in 2016).
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. Available online.
- Arthur E. Hutt, Seymour Bosworth, Douglas B. Hoyt. *Computer Security Handbook*. Wiley, 1995.