Cryptography

Basic elements of number theory

Marius Zimand

By default all the variables, such as a, b, k, etc., denote integer numbers.

Divisibility $a \neq 0$ divides b if $b = a \cdot k$ for some integer k.

Notation $a|b$.

Properties

1. $a \neq 0 \Rightarrow a|0$, $a|a$
2. $1|b$ for all b
3. $a|b$ and $b|c \Rightarrow a|c$
4. $a|b$ and $a|c \Rightarrow a|(sb + tc)$, for all integers s and t.

Prime Numbers

An integer number $p > 1$ is prime if it is divisible only by 1 and by itself.

Examples: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$

Facts:

- There are an infinity of prime numbers.
- **Fundamental Theorem of Arithmetic.** Each integer has a unique representation as a product of prime numbers.

  Example: $504 = 2^3 \cdot 3^2 \cdot 7$

- **Prime Number Theorem.** Let $\pi(x)$ denote the number of primes $\leq x$.

  For example $\pi(10) = 4$.

  Then $\pi(x) \approx \frac{x}{\ln x}$.

  The above means that

$$\lim_{x\to\infty} \frac{\pi(x)}{(x/\ln x)} = 1.$$

  In fact, it is known that if $x \geq 17$, then

$$\frac{x}{\ln x} < \pi(x) < 1.26\frac{x}{\ln x}.$$

  Application: Estimate the number of prime numbers with 100 digits.

  It is

$$\pi(10^{100}) - \pi(10^{99}) \approx \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \approx 3.9 \times 10^{97}.$$

- If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Greatest Common Divisor

Notation $gcd(a, b)$ or (a, b). It is what the name says it is: we look at the common divisors of a and b, and we pick the largest.

Examples: $gcd(6, 4) = 2$, $gcd(9, 14) = 1$, we say that 9 and 14 are relatively prime, or co-prime (the numbers have no common divisor other than 1).

How to find $gcd(a, b)$**?**

(1) Easy case: If we can factor a and b into primes. Then we take the common prime divisors at the smallest exponent.

$$\begin{aligned} 1728 &= 2^6 \cdot 3^3 \\ 405 &= 3^4 \cdot 5 \end{aligned}$$

So $gcd(1728, 405) = 3^3$.

(2) If a and b are large, it is very difficult to factor them. We use instead the Euclidean algorithm. First an example.

We want $gcd(482, 1180)$.

$$\begin{aligned} 1180 &= 2 \cdot 482 + 216 \\ 482 &= 2 \cdot 216 + 50 \\ 216 &= 4 \cdot 50 + 16 \\ 50 &= 3 \cdot 16 + 2 \qquad \text{(last non-zero remainder)} \\ 16 &= 8 \cdot 2 + 0. \end{aligned}$$

Note the shifts: remainder $\rightarrow$ divisor $\rightarrow$ dividend $\rightarrow$ discard.

In general

$$\begin{aligned} a &= q_1 \cdot b + r_1 \\ b &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k \cdot r_{k-1} + r_k \qquad \text{(last non-zero remainder)} \\ r_{k-1} &= q_{k+1} \cdot r_k + 0. \end{aligned}$$

Then $gcd(a, b) = r_k$.

Why is that? The answer is given by the following fact, which is easy to prove.

Fact 1 $gcd(a, b) = gcd(b, r_1)$.

So, $gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = \ldots = gcd(r_{k-1}, r_k) = r_k$.

It holds that $b > r_1 > r_2 > \ldots > r_k$, and all the numbers in the sequence are positive integer. Any decreasing sequence of positive integers is finite, so the algorithm will eventually stop. But how fast?

How fast is the euclidean algorithm?

Fact 2 *$r_3 < r_1/2$.*

Proof. Case 1. $r_2 \leq (r_1/2)$, then we are done because $r_3 < r_2$.

Case 2. $r_2 > (r_1/2)$. (Recall that $r_2 < r_1$.)

Then $q_3 = 1$, and $r_3 = r_1 - q_3 \cdot r_2 = r_1 - 1 \cdot r_2 < r_1 - (r_1/2) < (r_1/2)$.

In a similar way, we can show that $r_5 < (r_3/2)$, etc.

So we have $r_1 > 2r_3 > 4r_5 > \ldots > 2^n r_{2n+1}$ (the last odd step).

So, $2^n < \frac{r_1}{r_{2n+1}} \leq r_1 < b$.

So $n < \log_2(b)$.

Thus the number of steps is $\leq 2n + 2 < 2\log_2(b) + 2 = O(\log_2(b))$.

Thus the Euclidean Algorithm is very fast: the number of steps is roughly 2* length of b, and each step is essentially just a division.

Solving linear equation $ax + by = d$ in integers

We use the following theorem (stated without proof).

Theorem 3 *For any integers a and b there are integers x and y such that $ax + by = gcd(a, b)$.*

How to find x and y?

By using the *Extended Euclidean algorithm.*

Let $q_1, q_2, \ldots, q_n$ be the sequence of quotients in the Euclidean algorithm.

We form the recurrences:

$$x_0 = 0, x_1 = 1, x_j = -q_{j-1}x_{j-1} + x_{j-2},$$

and

$$y_0 = 1, y_1 = 0, y_j = -q_{j-1}y_{j-1} + y_{j-2}.$$

Then

$$ax_n + by_n = gcd(a, b).$$

Note: y_n is the coefficient of the larger between a and b.

In our example (i.e., gcd(482,1180)), we had:

$q_1 = 2, q_2 = 2, q_3 = 4, q_4 = 3, q_5 = 8.$

So, we get:

$x_0 = 0, x_1 = 1,$

$x_2 = -2x_1 + x_0 = -2$

$x_3 = -2x_2 + x_1 = 5$

$x_4 = -4x_3 + x_2 = -22$

$x_5 = -3x_4 + x_3 = 71.$

Similarly, we obtain $y_5 = -29$.

So $482 \cdot 71 + 1180 \cdot (-29) = 2 = gcd(480, 1180)$.

Now, back to the equation $ax + by = d$.

If $gcd(a, b) \not| d$, then there are no solutions.

Else find x' and y' such that $ax' + by' = gcd(a, b)$.

Then multiply x' and y' by $\frac{d}{gcd(a,b)}$ to obtain x and respectively y.

Modular Arithmetic

Definition 4 *$a = b(\text{mod } m)$ if $m|a - b$.*

Example: $32 = 2(\text{mod } 5)$, $-12 = 37(\text{mod } 7)$.

Equality mod m is an *equivalence relation*. An equivalence relation R is a binary relation that has the following three properties:

For all a in the domain, $R(a, a)$ (reflexivity).

For all a, b in the domain, if $R(a, b)$ then $R(b, a)$ (commutativity).

For all a, b, c in the domain, if $R(a, b)$ and $R(b, c)$, then $R(a, c)$ (transitivity).

If R is an equivalence relation, we can partition its domain into *equivalence classes*, where we put all the elements that are in the relation R in one class.

Thus, we can view the set of numbers that are equal to a modulo m as one single class. Such a class is called a *residue class*. We can pick a as the representative of that class. In this context, a intuitively denotes not one number but an entire set of numbers.

For example, if we work modulo 2, 0 denotes the class of even numbers, and 1 denotes the class of odd numbers. We say that 0 is a representative of the class of even numbers, and 1 is a representative of the class of odd numbers. One nice property is that we can add and multiply such classes by operating with their representatives.

Thus, to give just an example, one interpretation of the fact that $1 + 1 = 0(\text{mod } 2)$ is that

(any number in the class of 1) + (any number in the class of 1) = (some number in the class of 0).

And, similarly, one interpretation of the fact that $1 \times 0 = 0(\text{mod } 2)$ is that

(any number in the class of 1) $\times$ (any number in the class of 0) = (some number in the class of 0).

Or, in other words, to find how much is $a + b(\text{mod } m)$ (or $a \cdot b(\text{mod } m)$), one can take a representative a' of the class that contains a and one representative b' of the class that contains b and do the arithmetic operation using the representatives.

Integers modulo m can be added and multiplied. In some circumstances (to be discussed later) we can also do division modulo m.

For example: $3 + 5 = 2(\text{mod } 6)$, $4 + 2 = 0(\text{mod } 6)$, $4 + 5 = 3(\text{mod } 6)$.

We can form the addition table modulo 6.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Note that addition modulo 6

- is commutative (a+b = b+a).
- is associative (a+(b+c)) = ((a+b) + c)
- has a zero element (a+ zero = a)

- each element a has a symmetric element, which is denoted $-a$.

These properties are valid for addition modulo m, for any m (not just for $m = 6$).

We can also form the multiplication table modulo 6.

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Note that multiplication modulo 6

- is commutative (a × b = b × a).
- is associative (a ×(b ×c)) = ((a×b) × c)
- has a unity element (a × unity = a)

Note that not every element a has an inverse element, only 1 and 5 have inverses. In general,

Theorem 5 *a has an inverse modulo m iff $gcd(a, m) = 1$.*

Also note that row i has a period of length $\frac{6}{gcd(i,6)}$ and the entries on that row are multiples of $gcd(i, 6)$. This is true for any modulo m, not just for $m = 6$.

If the modulo m is a prime number, then all the elements $\neq 0$ have an inverse. In this case, we can do addition, multiplication, and division and have all the properties of these arithmetic operation (commutativity, assoc., distributivity or factoring-out) we are used to from elementary school.

Notation:

Z_m = class of residues modulo m with the operations of + and $\times$.

In general Z_m is a ring (+ has all the good properties, $\times$ is comm., assoc, has unity element, $\times$ is distributive with respect to +).

If m is prime, then Z_m is a field (a field has all the properties of a ring + one extra very important property: every element a, except 0, has an inverse, which is denoted a^{-1}; this basically implies that in a field, we can also do division).

How to find $a^{-1}(\text{mod } m)$**?**

Use the extended Euclidean algorithm to find s and t such that

$$as + mt = 1.$$

Then $as = 1(\text{mod } m)$, so $s = a^{-1}(\text{mod } m)$.

Solving $ax = b(\text{mod } n)$

Let $d = gcd(a, n)$.

Case 1. $d = 1$. Then we find $a^{-1}(\text{mod } n)$ (using the extended Euclidean Algorithm), and

$$x = b \cdot a^{-1}(\text{mod } n).$$

Example: $5x + 6 = 13(\text{mod } 11)$

$5x = 13 + (-6) = 7(\text{mod } 11)$

$x = 7 \cdot 5^{-1}(\text{mod } 11)$, $5^{-1} = 9$

So, $x = 7 \cdot 9 = 63 = 8(\text{mod } 11)$.

Case 2. If $d \not| b$, then the equation has no solution.

Case 3. $d|b$

We divide everything by d, and we get the new equation

$$\frac{a}{d} \cdot x = \frac{b}{d} (\text{mod } \frac{n}{d}).$$

Note that $gcd(\frac{a}{d}, \frac{n}{d}) = 1$, so we can solve the new equation as in Case 1.

So we solve the equation, and we obtain the solution x_0. The solutions of the original equation are

$$x_0, x_0 + \frac{n}{d}, x_0 + 2 \cdot \frac{n}{d}, \ldots, x_0 + (d-1) \cdot \frac{n}{d}.$$

Example:

$12x = 21(\text{mod } 39)$

$gcd(12, 39) = 3$, which divides 21.

New equations is (we divide everything by 3):

$4x = 7(\text{mod } 13)$

$x_0 = 7 \cdot (4^{-1}) = 7 \cdot 10 = 5(\text{mod } 13)$.

The solutions of the original equation are: 5, 5+13, 5+26, i.e, 5, 18, and 31.

The Chinese Remainder Theorem (CRT)

CRT is about solving a system of linear equations in modular arithmetic.

It is used to represent an integer as a sequence of smaller integers, or to break one congruence into several congruences with smaller moduli.

One simple example: If we know how much a number x is mod 42, then it is easy to determine how much it is mod 6 and mod 7.

$x = 25(\text{mod } 42) \Rightarrow x = 25 + 42k = 25 + (6k) \cdot 7 \Rightarrow x = 25(\text{mod } 7) = 4(\text{mod } 7)$

$\Rightarrow x = 25 + 42k = 25 + (7k) \cdot 6 \Rightarrow x = 25(\text{mod } 6) = 1(\text{mod } 6)$.

CRT goes the other way: Given the values of x mod 6 and mod 7, it allows us to fnd how much is x mod 42.

CRT - the simple form

Theorem 6 *Suppose $gcd(m, n) = 1$. Given a, b, the system of equations*

$$\begin{aligned} x &= a(\text{mod } m) \\ x &= b(\text{mod } n) \end{aligned}$$

has exactly one solution in the range $\{0, 1, \ldots, mn - 1\}$.

For example, consider the system of equations

$$\begin{aligned} x &= 3(\text{mod } 7) \\ x &= 5(\text{mod } 15) \end{aligned}$$

The CRT says that there exists such an x and just one such x among the integers $\{0, 1, \ldots, 7 \cdot 15 - 1 = 104\}$.

How to find such an x:

Case 1. If m and n are small.

We list the numbers that are $= b(\text{mod } n)$ (in our example, $= 5(\text{mod } 15)$)

$5, 20, 35, 50, 65, 80, 95$ (next one is ≥ 105)

Then we take each of the numbers in the list mod m (in our example, mod 7)

5, 6, 0, 1, 2, $\boxed{3}$, 4.

So the solution is 80.

Case 2. If m and n are big. In this case, the above procedure is not efficient, but we can use the same idea.

numbers $= b(\text{mod } n)$ are of the form $b + nk$.

So we need $b + nk = a(\text{mod } m)$ (here the unknown is k).

$nk = a - b(\text{mod } m)$

$gcd(m, n) = 1$, so $n^{-1}(\text{mod } m)$ exists.

So, $k = (a - b) \cdot n^{-1}(\text{mod } m)$.

Example: Solve

$$\begin{aligned} x &= 7(\text{mod } 12345) \\ x &= 3(\text{mod } 11111) \end{aligned}$$

$gcd(12345, 11111) = 1$ and $(11111)^{-1}(\text{mod } 12345) = 2471$.

So $k = 2471(7 - 3) = 9884(\text{mod } 12345)$.

So $x = 3 + 11111 \cdot 9884 = 109821127(\text{mod } 11111 \cdot 12345)$.

Why is CRT useful?

Example: Let's say we need to solve $x^2 = 1(\text{ mod } 35)$. It is easier to solve modular equations mod a prime number. 35 is not prime, but $35 = 5 \cdot 7$, so 35 is the product of two prime numbers.

Then

$$x^2 = 1(\text{mod } 35) \Leftrightarrow \begin{cases} x^2 = 1(\text{mod } 5) \\ x^2 = 1(\text{mod } 7) \end{cases}$$

" $\Rightarrow$" is clear.

" $\Leftarrow$": $(x^2 - 1) = 0(\text{mod } 5)$, $(x^2 - 1) = 0(\text{mod } 7)$, so $(x^2 - 1) = 0(\text{mod } 35)$ (a number that is a multiple of 5 and 7 has to be a multiple of 35).

So now we have two equations instead of one, but both are mod a prime number.

Lemma 7 *If p is a prime $\neq 2$, then $x^2 = 1(\text{ mod } p)$ has only the solutions 1 and -1.*

Proof. $x^2 - 1 = 0(\text{mod } p) \Leftrightarrow (x - 1)(x + 1) = 0(\text{mod } p)$, so $x - 1 = 0(\text{mod } p)$ or $x + 1 = 0(\text{mod } p)$ (because p is prime).

So, $x = \pm 1 (\text{mod } 5)$ and $x = \pm 1 (\text{mod } 7)$.

Now we want to go back to mod 35. For this we need the CRT!.

There are 4 cases.

$x = 1(\text{mod } 5), x = 1(\text{mod } 7) \overset{CRT}{\rightarrow} x = 1(\text{mod } 35)$

$x = 1(\text{mod } 5), x = -1(\text{mod } 7) \overset{CRT}{\rightarrow} x = 6(\text{mod } 35)$

$x = -1(\text{mod } 5), x = 1(\text{mod } 7) \overset{CRT}{\rightarrow} x = 29(\text{mod } 35)$

$x = -1(\text{mod } 5), x = -1(\text{mod } 7) \overset{CRT}{\rightarrow} x = 34(\text{mod } 35)$

(Please do the CRT implication at home, as an exercise.)

So $x^2 = 1(\text{mod } 35)$ has 4 solutions: 1, 6, 29, 34 (in the interval $\{0, 1, \ldots, 34\}$).

Chinese Remainder Theorem - general form

Let $m_1, m_2, \ldots, m_k$ be integers, pairwise relatively prime, i.e. $gcd(m_i, m_j) = 1$ for all $i \neq j$. For any integers $a_1, a_2, \ldots, a_k$ the system of equations

$$\begin{aligned} x &= a_1 (\text{mod } m_1) \\ x &= a_2 (\text{mod } m_2) \\ &\vdots \\ x &= a_k (\text{mod } m_k) \end{aligned}$$

has solutions, and moreover there exists exactly one solution in the interval $\{0, \ldots m_1 m_2 \ldots m_k - 1\}$.

Also note that there exists an efficient algorithm that finds the unique solution in the interval $\{0, \ldots m_1 m_2 \ldots m_k - 1\}$.

Modular exponentiation

We want to calculate $a^b (\text{mod } n)$

This is used a lot in crypto - in RSA both encryption and decryption are modular exponentiations.

Example: $2^{1234} (\text{mod } 789)$.

If we first calculate 2^{1234}, and then take the mod , we would have to work with numbers that are too large.

So we'll take the mod after each multiplication.

$2^{1234} = \underbrace{2 \times 2 \times \ldots \times 2}_{1233 \text{times}}$.

We can do fewer multiplications, if we do repeated squarings.

So we keep on squaring (everything is mod 789).

$2^2 = 4, 2^4 = 4^2 = 16$, $2^8 = 16^2 = 256$, $2^{16} = 256^2 = 49$, $2^{32} = 49^2 = 34$, $2^{64} = 367$, $2^{128} = 559$, $2^{256} = 37$, $2^{512} = 589$, $2^{1024} = 286$.

Next we note that $1234 = 1024 + 128 + 64 + 16 + 2$ (observe that $1234 = 10011010010_2$).

Therefore, $2^{1234} = 2^{1024} \cdot 2^{128} \cdot 2^{64} \cdot 2^{16} \cdot 2^2 = 286 \cdot 559 \cdot 367 \cdot 49 \cdot 4 = 481 (\text{mod } 789)$.

We can always do this - this is the repeated-squaring-with-mod method.

Suppose we want $a^b (\text{mod } n)$, and a, b, n have each 100 digits. So $b < 10^{100} = (10^3)^{33} \cdot 10 < (2^{10})^{33} \cdot 2^4 = 2^{334}$. So b in binary has < 334 bits. Thus, we need less than 334 squarings $a, a^2, a^4, \ldots$ and then less than 334 multiplications between these square numbers. So we do at most $2 \cdot 334 = 668$ multiplications and modulo reductions.

Fermat's Little Theorem and Euler Theorem

Theorem 8 (Fermat's Theorem.) *If p is a prime number and $p \not| a$, then $a^{p-1} = 1(\text{mod } p)$.*

Proof. Let $S = \{1, 2, 3, \ldots, p-1\}$. Let us consider the function $f(x) = a \cdot x(\text{ mod } p)$, defined for all $x \in S$.

Note that for all $x \in S$, $f(x) \in S$, because $f(x)$ cannot be 0

(Proof by contradiction: assume $f(x) = 0$, i.e., $ax = 0$, so $x = a^{-1}0 = 0$, so x is not in S, contradiction. Note that a^{-1} exists because $a \neq 0(\text{mod } p)$).

Also note that if $x \neq y(\text{mod } p)$, then $ax \neq ay(\text{mod } p)$.

(because if $ax = ay(\text{mod } p)$, then we can multiply on both sides by a^{-1} and we obtain $x = y(\text{mod } p)$, contradiction.)

So $a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$ are the same as $1, 2, \ldots, (p-1)$, perhaps in a different order.

Then $(a \cdot 1) \cdot (a \cdot 2) \cdot \ldots \cdot (a \cdot (p-1)) = 1 \cdot 2 \cdot \ldots \cdot (p-1)(\text{mod } p)$.

So, $a^{p-1} \cdot (1 \cdot 2 \cdot \ldots \cdot (p-1)) = (1 \cdot 2 \cdot \ldots \cdot (p-1))(\text{mod } p)$.

Now we divide both sides by $(1 \cdot 2 \cdot \ldots \cdot (p-1))$ (why is it ok to divide?) and we obtain that $a^{p-1} = 1(\text{mod } p)$.

Example: $2^{10} = 1(\text{mod } 11)$

$2^{53} =?(\text{mod } 11)$

$2^{53} = (2^{10})^5 \cdot 2^3 = 1 \cdot 8(\text{mod } 11) = 8(\text{mod } 11)$.

Let's consider now that we work modulo n and n is not a prime number.

$\phi(n)$ = number of integers between 1 and n that are relatively prime with n.

Ex: $n = 10$, $\phi(10) = 4$, because $1, 3, 7, 9$ are all the numbers less than 10 that are relatively prime with 10.

$\phi(n)$ is called the Euler's ϕ function.

If p is prime, $\phi(p) = (p-1)$.

$\phi(p^r) = p^r - p^{r-1} = (1 - \frac{1}{p}) \cdot p^r$.

In general, for any integer n, $\phi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$.

Theorem 9 (Euler's Theorem) *If* $gcd(a, n) = 1$, *then* $a^{\phi(n)} = 1 (\text{mod } n)$.

Example: what are the last 3 digits of 7^{803}?

We need $7^{803} (\text{mod } 1000)$. $\phi(1000) = 1000(1 - 1/2)(1 - 1/5) = 400$.

So $7^{400} = 1 (\text{mod } 1000)$.

Then $7^{803} = 7^{400} \cdot 7^{400} \cdot 7^3 = 1 \cdot 1 \cdot 343 = 343 (\text{mod } 1000)$.

So, we have the following principle, which will be used a lot.

When we work mod n, we can reduce the exponent mod $\phi(n)$.

So when we do modular arithmetic mod n, we can reduce in the base mod n and in the exponent mod $\phi(n)$.

Primitive Roots (also called generators)

Let us look at the powers of 3 modulo 7.

$$3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1,$$

after which, of course, they start to repeat.

We have obtained $\{1, 2, 3, 4, 5, 6\}$, all the non-zero residues modulo 7.

3 is said to be a primitive root mod 7 (or a generator mod 7).

Definition 10 *If* p *is a prime number, a primitive root* mod p *is a number whose powers yield every nonzero residue* mod p.

Properties:

- if g is a primitive root mod p, then $g^n = 1 (\text{mod } p)$ iff $n = 0 (\text{mod } p-1)$.
- if g is a primitive root mod p, then

$$g^j = g^k (\text{mod } p) \text{ iff } j = k (\text{mod } p-1).$$

- there are $\phi(p-1)$ primitive roots mod p.

Square roots mod n

Problem: Solve the equation $x^2 = b (\text{mod } n)$.

We'll consider the cases:

(1) n is a prime number, and

(2) $n = p \cdot q$, with p and q primes.

Case (1) is easy to solve.

Regarding case (2): It is computationally equivalent to factoring in the following sense:

(A) the equation can be solved fast if we know the factorization of n, and,

(B) conversely, if we know the solutions, then we can factor fast the number n.

Case 1. $n = p$, p prime. There are two possibilities: $p = 1 (\text{mod } 4)$ and $p = 3 (\text{mod } 4)$.

The subcase $p = 1 (\text{mod } 4)$: there is an efficient algorithm that solves the equation. (I will not present the algorithm; can be found in the literature, ask me for references).

The subcase $p = 3 (\text{mod } 4)$: It is even easier, because the solutions can be found with a simple formula.

Proposition 11 *Let $p = 3(\text{mod } 4)$ be a prime. let b be an integer, $b \neq 0(\text{mod } p)$. Then one and only one of b and $-b$ is a square and the square roots (of the one who is a square) are $x = \pm b^{(p+1)/4}$.*

The proof is not hard, but we'll skip it.

Example:

(a) Find the sqrt of $5(\text{mod } 11)$.

$11 = 4 \cdot 2 + 3$, so $11 = 3(\text{mod } 4)$, so we can use the proposition.

We compute $5^{(11+1)/4} = 5^3 = 4(\text{mod } 11)$.

Since $4^2 = 5(\text{mod } 11)$, 5 is a square and the sqrt are 4 and $-4 = 7(\text{mod } 11)$.

(b) Find the sqrt of $2(\text{mod } 11)$.

We can use the proposition, for the same reason.

We compute $2^{(11+1)/4} = 2^3 = 8(\text{mod } 11)$.

But $8^2 = 64 = 9 \neq 2(\text{mod } 11)$, so 8 is a sqrt of -2, and 2 is not a square $(\text{mod } 11)$.

Case 2: $n = p \cdot q$, with p and q primes.

If we know p and q, then it's easy to solve the equation. The key is to use CRT (and actually we have seen the method when we discussed CRT).

Example: $x^2 = 71(\text{mod } 77)$. Note that $77 = 7 \cdot 11$.

We have: $x^2 = 71 = 1(\text{mod } 7)$ and $x^2 = 71 = 5(\text{mod } 11)$.

Using case 1, we solve the two equations and we obtain:

$$x = \pm 1(\text{mod } 7) \text{ and } x = \pm 4(\text{mod } 11).$$

Now we use the CRT, and we get 4 solutions: $x = \pm 15, \pm 29(\text{mod } 77)$.

The conclusion is that if we can factor n and get p and q, then we can find the 4 solutions of the equation $x^2 = b(\text{mod } n)$.

Now we prove statement (B). Suppose we can find the 4 solutions of the equation $x^2 = b(\text{mod } n)$, where $b \neq 0$. We show that having this information allows us to factor n fast.

Let the 4 solutions be $\pm a$ and $\pm c$, with $a \neq \pm c$.

So $a^2 = c^2(\text{mod } n)$.

Then $a^2 - c^2 = 0(\text{ mod } n)$, so $(a+c)(a-c) = 0(\text{ mod } n)$, so $(a+c)(a-c) = k \cdot p \cdot q$, for some integer k.

Then p must divide $(a+c)$ or $(a-c)$ (because p is prime). Let's say that p divides $(a+c)$ (the other case is similar).

It cannot be that q also divides $(a+c)$, because otherwise $(a+c) = 0(\text{mod } n)$, which is not true (because $a \neq -c(\text{mod } n)$).

Therefore $gcd(a+c, n) = p$. Consequently we can use the Euclidean algorithm and find p (and after that q).

Thus we have established the following:

Let $n = p \cdot q$, with p and q primes, and let $b \neq 0(\text{mod } n)$.

Then finding the four solutions of the equation $x^2 = b(\text{ mod } n)$ is *computationally equivalent* to factoring n.

Computationally equivalent: if we can do one of them efficiently, we can do the other one efficiently as well.

Formally we have shown that SQUARE-ROOT is polynomial-time reducible to FACTORING, and vice-versa, FACTORING is polynomial-time reducible to SQUARE-ROOT.

Since we believe that factoring n is very hard, the above implies that solving $x^2 = b(\text{mod } n)$ is probably also very hard.