Lecture 7. Number Theory

DR. YARASLAU ZADVORNY

One More Trick: Euclid's Algorithm

Suppose a, b are two natural numbers and we have to find their greatest common divisor.

The algorithm is based on the following

Statement. If $a > b$ then $\gcd(a, b) = \gcd(a - b, b)$.

One More Trick: Euclid's Algorithm

Statement. If $a > b$ then $\gcd(a, b) = \gcd(a - b, b)$.

Thus, we have the following algorithm:

$$\gcd(2057, 663) = \gcd(1394, 663) = \gcd(731, 663) = \gcd(68, 663) =$$

$$= \gcd(68, 595) = \gcd(68, 527) = \gcd(68, 459) = \gcd(68, 391) = \gcd(68, 323) =$$

$$= \gcd(68, 255) = \gcd(68, 187) = \gcd(68, 119) = \gcd(68, 51) = \gcd(17, 51) =$$

$$= \gcd(17, 34) = \gcd(17, 17) = 17.$$

One More Trick: Euclid's Algorithm

Statement. If $a > b$ then $\gcd(a, b) = \gcd(a - b, b)$.

Thus, we have the following algorithm:

$$\gcd(2057, 663) = \gcd(1394, 663) = \gcd(731, 663) = \gcd(68, 663) =$$

$$= \gcd(68, 595) = \gcd(68, 527) = \gcd(68, 459) = \gcd(68, 391) = \gcd(68, 323) =$$

$$= \gcd(68, 255) = \gcd(68, 187) = \gcd(68, 119) = \gcd(68, 51) = \gcd(17, 51) =$$

$$= \gcd(17, 34) = \gcd(17, 17) = 17.$$

We can do it quicker. For example, here we subtract 68 from 663, while the obtained number is greater than 68. Obviously, we finally get the remainder of the number 663 modulo 68.

One More Trick: Euclid's Algorithm

Statement. If $a > b$ then $\gcd(a, b) = \gcd(a - b, b)$.

Thus, we have the following algorithm:

$$\gcd(2057, 663) = \gcd(68, 663) = \gcd(68, 51) = \gcd(17, 51) = 17.$$

We can do it quicker. For example, here we subtract 68 from 663, while the obtained number is greater than 68. Obviously, we finally get the remainder of the number 663 modulo 68.

Euclid's Algorithm: One Important Application

Suppose we need to find such x that $38x \equiv 53 \pmod{101}$.

In other words, we have to find such x that

$$38x = 101k + 53.$$

Let us find such y that

$$38y = 101m + 1.$$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$$101 = 38 \times 2 + 25$$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$$101 = 38 \times 2 + 25$$

$$38 = 25 \times 1 + 13$$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$$101 = 38 \times 2 + 25$$

$$38 = 25 \times 1 + 13$$

$$25 = 13 \times 1 + 12$$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$$101 = 38 \times 2 + 25$$

$$38 = 25 \times 1 + 13$$

$$25 = 13 \times 1 + 12$$

$$13 = 12 \times 1 + 1$$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$101 = 38 \times 2 + 25$

$38 = 25 \times 1 + 13$

$25 = 13 \times 1 + 12$

$13 = 12 \times 1 + 1$ $\qquad$ $1 = 13 \times 1 - 12 \times 1$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$101 = 38 \times 2 + 25$

$38 = 25 \times 1 + 13$

$25 = 13 \times 1 + 12$ $\qquad$ $12 = 25 \times 1 - 13 \times 1$

$13 = 12 \times 1 + 1$ $\qquad$ $1 = 13 \times 1 - 12 \times 1$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$101 = 38 \times 2 + 25$

$38 = 25 \times 1 + 13$ $\quad$ $13 = 38 \times 1 - 25 \times 1$

$25 = 13 \times 1 + 12$ $\quad$ $12 = 25 \times 1 - 13 \times 1$

$13 = 12 \times 1 + 1$ $\quad$ $1 = 13 \times 1 - 12 \times 1$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$101 = 38 \times 2 + 25$ $\quad$ $25 = 101 \times 1 - 38 \times 2$

$38 = 25 \times 1 + 13$ $\quad$ $13 = 38 \times 1 - 25 \times 1$

$25 = 13 \times 1 + 12$ $\quad$ $12 = 25 \times 1 - 13 \times 1$

$13 = 12 \times 1 + 1$ $\quad$ $1 = 13 \times 1 - 12 \times 1$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$101 = 38 \times 2 + 25$ $\quad$ $25 = 101 \times 1 - 38 \times 2$

$38 = 25 \times 1 + 13$ $\quad$ $13 = 38 \times 1 - 25 \times 1$

$25 = 13 \times 1 + 12$ $\quad$ $12 = 25 \times 1 - 13 \times 1$

$13 = 12 \times 1 + 1$ $\quad$ $1 = 13 \times 1 - 12 \times 1$ $\quad$ $1 = 13 \times 1 - 12 \times 1 =$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$101 = 38 \times 2 + 25$ $\quad 25 = 101 \times 1 - 38 \times 2$

$38 = 25 \times 1 + 13$ $\quad 13 = 38 \times 1 - 25 \times 1$

$25 = 13 \times 1 + 12$ $\quad 12 = 25 \times 1 - 13 \times 1$ $\quad = 13 \times 1 - (25 \times 1 - 13 \times 1) = 13 \times 2 - 25 \times 1 =$

$13 = 12 \times 1 + 1$ $\quad 1 = 13 \times 1 - 12 \times 1$ $\quad 1 = 13 \times 1 - 12 \times 1 =$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$101 = 38 \times 2 + 25$ $\quad$ $25 = 101 \times 1 - 38 \times 2$

$38 = 25 \times 1 + 13$ $\quad$ $13 = 38 \times 1 - 25 \times 1$ $\quad$ $= (38 \times 1 - 25 \times 1) \times 2 - 25 \times 1 = 38 \times 2 - 25 \times 3 =$

$25 = 13 \times 1 + 12$ $\quad$ $12 = 25 \times 1 - 13 \times 1$ $\quad$ $= 13 \times 1 - (25 \times 1 - 13 \times 1) = 13 \times 2 - 25 \times 1 =$

$13 = 12 \times 1 + 1$ $\quad$ $1 = 13 \times 1 - 12 \times 1$ $\quad$ $1 = 13 \times 1 - 12 \times 1 =$

Euclid's Algorithm: One Important Application

Let us find such y that

$$38y = 101m + 1.$$

We apply the Euclid's algorithm:

$101 = 38 \times 2 + 25$ $\quad$ $25 = 101 \times 1 - 38 \times 2$ $\quad$ $= 38 \times 2 - (101 \times 1 - 38 \times 2) \times 3 = 38 \times 8 - 101 \times 3$

$38 = 25 \times 1 + 13$ $\quad$ $13 = 38 \times 1 - 25 \times 1$ $\quad$ $= (38 \times 1 - 25 \times 1) \times 2 - 25 \times 1 = 38 \times 2 - 25 \times 3 =$

$25 = 13 \times 1 + 12$ $\quad$ $12 = 25 \times 1 - 13 \times 1$ $\quad$ $= 13 \times 1 - (25 \times 1 - 13 \times 1) = 13 \times 2 - 25 \times 1 =$

$13 = 12 \times 1 + 1$ $\quad$ $1 = 13 \times 1 - 12 \times 1$ $\quad$ $1 = 13 \times 1 - 12 \times 1 =$

Euclid's Algorithm: One Important Application

Suppose we need to find such x that $38x \equiv 53 \pmod{101}$.

In other words, we have to find such x that

$$38x = 101k + 53.$$

Let us find such y that

$$38y = 101m + 1.$$

Thus $y = 8$, $m = 3$. We multiply these numbers by 53 and get

$$x = 424,\ k = 159.$$

We can also notice that $424 \equiv 20 \pmod{101}$ and take

$$x = 20.$$

Euler's Totient Function

The Euler's totient function, $\varphi(n)$, is the number of naturals which are smaller than n and are relatively prime to it.

Let us, for example, calculate $\varphi(20)$:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

Euler's Totient Function

The Euler's totient function, $\varphi(n)$, is the number of naturals which are smaller than n and are relatively prime to it.

Let us, for example, calculate $\varphi(20)$:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

Euler's Totient Function

The Euler's totient function, $\varphi(n)$, is the number of naturals which are smaller than n and are relatively prime to it.

Let us, for example, calculate $\varphi(20)$:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

Euler's Totient Function

The Euler's totient function, $\varphi(n)$, is the number of naturals which are smaller than n and are relatively prime to it.

Let us, for example, calculate $\varphi(20)$:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

So $\varphi(20) = 8$.

Euler's Totient Function: Properties

1) If p is prime then $\varphi(p) = p - 1$.

Indeed, if p is prime then any natural which is smaller than p is coprime to it.

Euler's Totient Function: Properties

1) If p is prime then $\varphi(p) = p - 1$.

Indeed, if p is prime then any natural which is smaller than p is coprime to it.

2) If p is prime then $\varphi(p^n) = p^n - p^{n-1}$.

Indeed, if p is prime then a natural is coprime to p^n if and only if it is not divisible by p. Thus, there are exactly $p^{n-1} - 1$ number which are smaller than p^n and are **not** coprime to it. Thus

$$\varphi(p^n) = (p^n - 1) - (p^{n-1} - 1) = p^n - p^{n-1}.$$

Euler's Totient Function: Properties

2) If p is prime then $\varphi(p^n) = p^n - p^{n-1}$.

Now, to calculate $\varphi(n)$ it is enough to prove the next property:

3) $\varphi(n)$ is a multiplicative function, that is, $\varphi(nm) = \varphi(n) \times \varphi(m)$ if $\gcd(n, m) = 1$.

Euler's Totient Function: Properties

2) If p is prime then $\varphi(p^n) = p^n - p^{n-1}$.

Now, to calculate $\varphi(n)$ it is enough to prove the next property:

3) $\varphi(n)$ is a multiplicative function, that is, $\varphi(nm) = \varphi(n) \times \varphi(m)$ if $\gcd(n, m) = 1$.

$$\varphi(72000) = \varphi(2^6 \times 3^2 \times 5^3) = \varphi(2^6) \times \varphi(3^2) \times \varphi(5^3) =$$

$$= (2^6 - 2^5) \times (3^2 - 3^1) \times (5^3 - 5^2) = 32 \times 6 \times 100 = 19200.$$

Euler's Totient Function: Properties

Let $m = 10$, $n = 9$. Then $\varphi(90) = \varphi(10) \times \varphi(9) = 4 \times 6$.

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	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90

Euler's Totient Function: Properties

Let $m = 10$, $n = 9$. Then $\varphi(90) = \varphi(10) \times \varphi(9) = 4 \times 6$.

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	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90

Euler's Totient Function: Properties

Let $m = 10$, $n = 9$. Then $\varphi(90) = \varphi(10) \times \varphi(9) = 4 \times 6$.

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	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90

Euler's Totient Function: Properties

How does it work in general? Let us see.

In a column, there are numbers which give the same remainder modulo m. Thus, all the numbers in the same column are at the same time coprime or not coprime to m. Moreover, there are exactly $\varphi(m)$ columns such that the numbers in them are coprime to m.

1	2	3	…	$m-3$	$m-2$	$m-1$	m
$m+1$	$m+2$	$m+3$	…	$2m-3$	$2m-2$	$2m-1$	$2m$
$2m+1$	$2m+2$	$2m+3$	…	$3m-3$	$3m-2$	$3m-1$	$3m$
			…				
$(n-1)m+1$	$(n-1)m+2$	$(n-1)m+3$		$nm-3$	$nm-2$	$nm-1$	nm

Euler's Totient Function: Properties

How does it work in general? Let us see.

In a column, there are numbers which give the same remainder modulo m. Thus, all the numbers in the same column are at the same time coprime or not coprime to m. Moreover, there are exactly $\varphi(m)$ columns such that the numbers in them are coprime to m.

We also have to prove that in each column, there are exactly $\varphi(n)$ numbers which are coprime to n.

1	2	3	…	$m-3$	$m-2$	$m-1$	m
$m+1$	$m+2$	$m+3$	…	$2m-3$	$2m-2$	$2m-1$	$2m$
$2m+1$	$2m+2$	$2m+3$	…	$3m-3$	$3m-2$	$3m-1$	$3m$
			…				
$(n-1)m+1$	$(n-1)m+2$	$(n-1)m+3$		$nm-3$	$nm-2$	$nm-1$	nm

Euler's Totient Function: Properties

3

$m + 3$

$2m + 3$

$(n - 1)m + 3$

We are going to prove that the numbers in the column give different residues modulo n. Thus, exactly $\varphi(n)$ of these numbers give the residues that are coprime to n; thus, exactly $\varphi(n)$ of them are coprime to n.

Euler's Totient Function: Properties

3

$m + 3$

$2m + 3$

$(n-1)m + 3$

We are going to prove that the numbers in the column give different residues modulo n. Thus, exactly $\varphi(n)$ of these numbers give the residues that are coprime to n; thus, exactly $\varphi(n)$ of them are coprime to n.

Suppose there are two numbers, $km + 3$ and $lm + 3$, where $0 \le k < l < n$, which give the same residues modulo n. Then

$$lm - km \vdots n, m(l-k) \vdots n, l-k \vdots n,$$

which is impossible since $0 \le k < l < n$ and thus $0 < l - k < n$.

Euler's Theorem

Let a and m be integers which are coprime. Then

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

Prove. Suppose $r_1, r_2, \ldots, r_{\varphi(m)}$ are residues modulo m. Consider the numbers

$$ar_1, ar_2, \ldots, ar_{\varphi(m)}.$$

Let's take the product of these numbers:

$$ar_1 \times ar_2 \times \ldots \times ar_{\varphi(m)} = a^{\varphi(m)}\, r_1 r_2 \ldots r_{\varphi(m)} \equiv r_1 r_2 \ldots r_{\varphi(m)} \pmod{m}.$$

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

RSA-Cryptosystem

It is well-known that any text can be considered as a number, say, x.

The main idea is to choose two numbers, e and m, and to encrypt the text x using the formula

$$y \equiv x^e \pmod{m}.$$

RSA-Cryptosystem

It is well-known that any text can be considered as a number, say, x.

The main idea is to choose two numbers, e and m, and to encrypt the text x using the formula

$$y \equiv x^e \pmod{m}.$$

How to decode? Suppose d is such a natural that

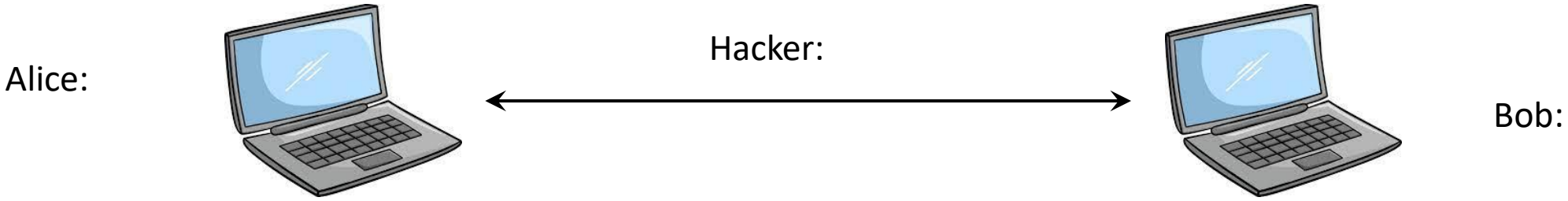
$$de \equiv 1 \pmod{\varphi(m)}.$$

Then

$$y^d \equiv (x^e)^d \equiv x^{de} \equiv x^{k\varphi(m)+1} \equiv (x^{\varphi(m)})^k \times x \equiv x \pmod{m}.$$

RSA-Cryptosystem

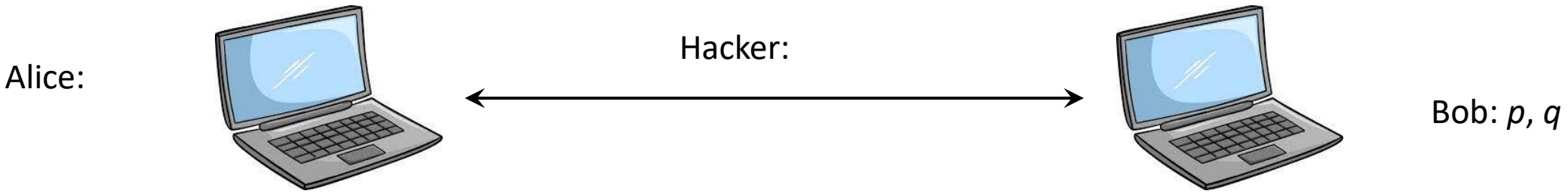
Suppose Alice wants to write an encrypted message to Bob.



RSA-Cryptosystem

Suppose Alice wants to write an encrypted message to Bob.

To organize the RSA-cryptosystem, Bob chooses two big primes, p and q. He



RSA-Cryptosystem

Suppose Alice wants to write an encrypted message to Bob.

To organize the RSA-cryptosystem, Bob chooses two big primes, p and q. He

takes $m = pq$,

Alice:

Hacker:

Bob: p, q, m

RSA-Cryptosystem

Suppose Alice wants to write an encrypted message to Bob.

To organize the RSA-cryptosystem, Bob chooses two big primes, p and q. He

takes $m = pq$,

finds $\varphi(m) = (p - 1)(q - 1)$.

Alice:

Hacker:

Bob: p, q, m, $\varphi(m)$

RSA-Cryptosystem

Suppose Alice wants to write an encrypted message to Bob.

To organize the RSA-cryptosystem, Bob chooses two big primes, p and q. He

takes $m = pq$,

finds $\varphi(m) = (p - 1)(q - 1)$.

chooses such e which is coprime to $\varphi(m) = (p - 1)(q - 1)$

Alice:

Hacker:

Bob: p, q, m, $\varphi(m)$, e

RSA-Cryptosystem

Suppose Alice wants to write an encrypted message to Bob.

To organize the RSA-cryptosystem, Bob chooses two big primes, p and q. He

takes $m = pq$,

finds $\varphi(m) = (p - 1)(q - 1)$.

chooses such e which is coprime to $\varphi(m) = (p - 1)(q - 1)$

and d such that $de \equiv 1 \pmod{\varphi(m)}$.

Alice:

Hacker:

Bob: p, q, m, $\varphi(m)$, e, d

RSA-Cryptosystem

Suppose Alice wants to write an encrypted message to Bob.

To organize the RSA-cryptosystem, Bob chooses two big primes, p and q. He

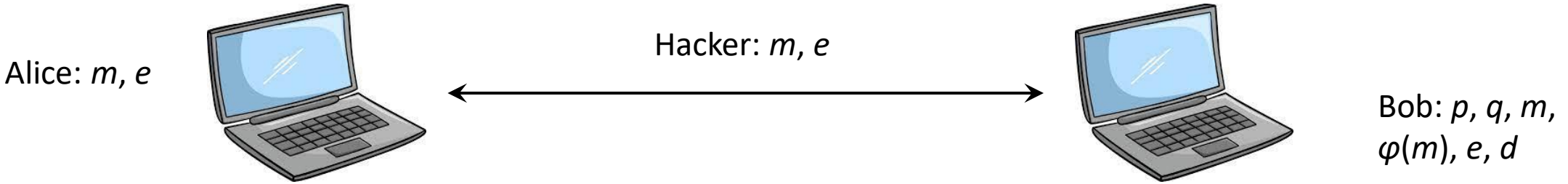
takes $m = pq$,

finds $\varphi(m) = (p - 1)(q - 1)$.

chooses such e which is coprime to $\varphi(m) = (p - 1)(q - 1)$

and d such that $de \equiv 1 \pmod{\varphi(m)}$.

Then he sends the numbers m and e to Alice, but the numbers m, p and q are still secret.



RSA-Cryptosystem

So:

the numbers m and e are well-known; the numbers p, q and d are secret.

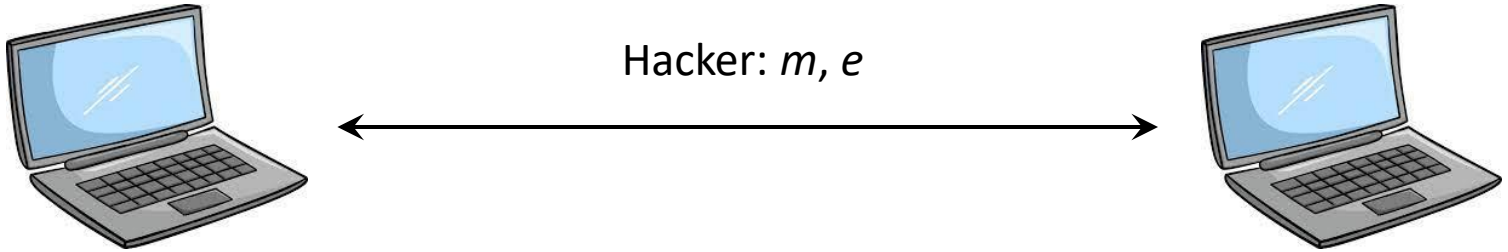
If Alice wants to encrypt the message x she simply finds

$$y \equiv x^e \pmod{m}.$$

If Bob wants to decode the message y he finds

$$y^d \equiv x \pmod{m}.$$

Alice: m, e



Bob: p, q, m, $\varphi(m)$, e, d

RSA-Cryptosystem

So:

the numbers m and e are well-known; the numbers p, q and d are secret.

If Alice wants to encrypt the message x she simply finds

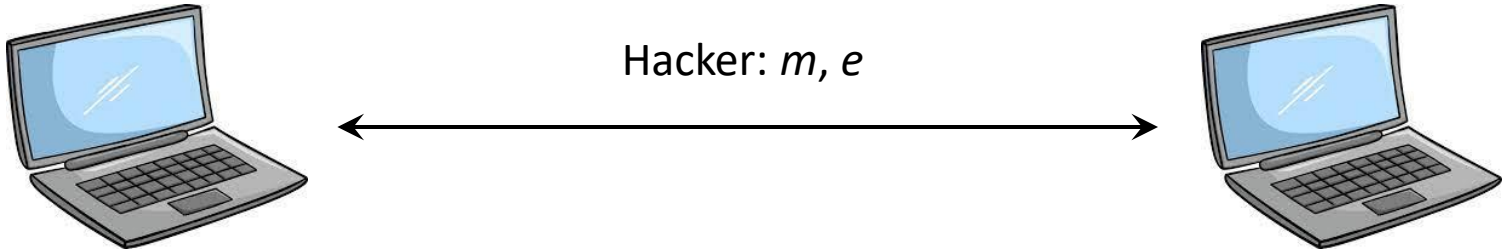
$$y \equiv x^e \pmod{m}.$$

If Bob wants to decode the message y he finds

$$y^d \equiv x \pmod{m}.$$

Suppose a hacker wants to decode the message y. But he doesn't know the number d!!!

Alice: m, e



Bob: p, q, m, $\varphi(m)$, e, d

Exponentiation by squaring

There is still a question: how fast can we find $y \equiv x^e \pmod{m}$?

We do not need do multiply x by itself e times. For example, to find x^{1541} we do the following:

represent 1541 as a sum of powers of 2:

$$1541 = 1024 + 512 + 4 + 1 = 2^{10} + 2^9 + 2^2 + 2^0;$$

by calculating a square find

$$x, x^2, x^4, x^8, x^{16}, x^{32}, x^{64}, x^{128}, x^{256}, x^{512}, x^{1024}.$$

Now we need to find

$$x^{1541} = x^{1024} \times x^{512} \times x^4 \times x^1.$$

Fermat primality test

Suppose Bob has a big number n and he wants to check if it is prime.

He can do the following:

take a number a which is not divisible by n;

check if it is true that

$$a^{n-1} \equiv 1 \pmod{n}.$$

If it is not so then n is not a prime.

If it is so you can repeat the test several times.

Carmichael numbers

A Carmichael number is such a composite number n that for any a which is coprime to n

$$a^{n-1} \equiv 1 \pmod{n}.$$

Such a number cannot be proved to be composite using the Fermat primality test.

For example, take $n = 561 = 3 \times 11 \times 17$:

$$a^{560} \equiv (a^2)^{280} \equiv 1^{280} \equiv 1 \pmod{3};$$

$$a^{560} \equiv (a^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{11};$$

$$a^{560} \equiv (a^{16})^{35} \equiv 1^{35} \equiv 1 \pmod{17}.$$

So $a^{560} - 1$ is divisible by 3, 11 and 17; thus, it is also divisible by 561 and

$$a^{560} \equiv 1 \pmod{561}.$$