Number Theory and Cryptography

- Prime number (has exactly 2 divisors: 1 and itself)
- The fundamental theorem of arithmetic: every integer greater than 1 either is a prime number itself, or can be represented as the product of prime numbers, and this representation is unique, up to the order of the factors.
- Relatively prime numbers: there is no integer greater than one that divides both of them.

Euclid's Algorithm

For two positive integers a, b:

function $\gcd(a, b)$

    if $a = b$ **then return** a

    if $a < b$ **then** $\text{swap}(a, b)$

    return $\gcd(a - b, b)$

GCD(a,b)

Theorem: Let $a > b$. Then $\gcd(a, b) = \gcd(a - b, b)$.

Proof:

The theorem follows from the following claim: x is a common divisor of a and b if and only if x is a common divisor of $a - b$ and b.

($\Rightarrow$) Suppose that x is a common divisor of a and b. Then $a = \alpha x$ and $b = \beta x$ for some integers α, β.

Therefore $a - b = \alpha\, x - \beta x = (\alpha\ - \beta)x$, so x is a divisor of $a - b$.

($\Leftarrow$) Suppose now that x is a common divisor of $a - b$ and b.

Then $a - b = \gamma x$ and $b = \delta x$ for some integers γ, δ. This implies that $a = (a - b) + b = \gamma x + \delta x = (\gamma + \delta)x$, so x is a divisor of a.

GCD as a Linear Combination
Extended Euclidean Algorithm

Theorem: If a, b are positive integers, then there exist integers α, β such that $\gcd(a, b) = \alpha a + \beta b$.

For small numbers a, b, one can simply list all multiples of a and b, until finding those, whose difference is c = gcd(a, b).

The Extended Euclidean Algorithm

Step 1: The (usual) Euclidean algorithm:

$$
\begin{aligned}
(1) \qquad 65 &= 1 \cdot 40 + \boxed{25} \\
(2) \qquad 40 &= 1 \cdot \boxed{25} + 15 \\
(3) \qquad \boxed{25} &= 1 \cdot 15 + 10 \\
(4) \qquad 15 &= 1 \cdot 10 + 5 \\
\qquad\quad 10 &= 2 \cdot 5
\end{aligned}
$$

Therefore: $\gcd(65, 40) = 5$.

Theorem: If a, b are positive integers then there exist integers α, β such that $\gcd(a, b) = \alpha a + \beta b$.

http://www.mast.queensu.ca/~math418/m418oh/m418oh04.pdf

The Extended Euclidean Algorithm

$\mathbf{gcd(a, b) = \alpha a + \beta b}$

Step 1: The (usual) Euclidean algorithm:

$$
\begin{aligned}
(1) \qquad 65 &= 1 \cdot 40 + \boxed{25} \\
(2) \qquad 40 &= 1 \cdot \boxed{25} + 15 \\
(3) \qquad \boxed{25} &= 1 \cdot 15 + 10 \\
(4) \qquad 15 &= 1 \cdot 10 + 5 \\
10 &= 2 \cdot 5
\end{aligned}
$$

Therefore: $\gcd(65, 40) = 5$.

Step 2: Using the method of back-substitution:

$$
\begin{aligned}
5 \overset{(4)}{=} 15 - 10 & \\
\overset{(3)}{=} 15 - (25 - 15) &= 2 \cdot 15 - 25 \\
\overset{(2)}{=} 2(40 - 25) - 25 &= 2 \cdot 40 - 3 \cdot 25 \\
\overset{(1)}{=} 2 \cdot 40 - 3(65 - 40) &= 5 \cdot 40 - 3 \cdot 65
\end{aligned}
$$

Conclusion: $65(-3) + 40(5) = 5$.

http://www.mast.queensu.ca/~math418/m418oh/m418oh04.pdf

Modular Arithmetic

Let $m > 0$ be a positive integer (called the modulus). Two integers a and b are congruent modulo m if $b - a$ is divisible by m:

$$a \equiv b \pmod{m} \leftrightarrow a - b = m \cdot k \quad \text{for some int. } k.$$

Ex. 1. $24 \equiv 4 \pmod{10}$ because $24 - 4 = 10 \cdot 2$.

Ex. 2. Prove that there is no integer x satisfying

$$106x \equiv 9 \pmod{284}$$

Modular Arithmetic

Computation Rules for Mod Arithmetic

1) $(a + b)\ rem\ m = (a\ rem\ m) + (b\ rem\ m)$
2) $(a - b)\ rem\ m = (a\ rem\ m) - (b\ rem\ m)$
3) $(a * b)\ rem\ m = (a\ rem\ m) * (b\ rem\ m)$

Modular Arithmetic

Exponentiation (by squaring):

$$3^{17} \text{ rem } 5 \equiv 3^{16} \cdot 3 \text{ rem } 5 \equiv (3^2)^8 \cdot 3 \text{ rem } 5 \equiv$$

$$9^8 \cdot 3 \text{ rem } 5 \equiv 4^8 \cdot 3 \text{ rem } 5 \equiv (4^2)^4 \cdot 3 \text{ rem } 5 \equiv$$

$$16^4 \cdot 3 \text{ rem } 5 \equiv 1^4 \cdot 3 \text{ rem } 5 \equiv 3$$

Inverses Modulo a Prime

An **inverse** of a modulo m is an integer b such that

$$ab \equiv 1 \pmod{m}$$

Theorem

Let p be a prime and $y \in \{1, 2, \ldots, p - 1\}$. Then the multiplic. inverse of y modulo p exists and is unique (among numbers between 1 and $p - 1$).

Existence.

Recall Extended Euclidean Algorithm: $\alpha y + \beta p = gcd(y,p)$.

Since y and p are relatively prime, $gcd(y,p) = 1$, and $\alpha y + \beta p = 1$.

Then $\alpha y + \beta p \equiv 1 \pmod{p}$; $\alpha y \equiv 1 \pmod{p}$,

and $\boldsymbol{\alpha}$ is a multiplicative inverse of y.

Uniqueness.

By contradiction

Required

Inverses

$10^{-1} = 1 \pmod 9$,
since $10 \cdot 1 \equiv 1 \pmod 9$,

$10^{-1} \equiv ? \pmod 8$

10^{-1} does not have an inverse modulo 8 :
$10 \cdot a \equiv 1 \pmod 8$ means
$10 \cdot a = 8 \cdot b + 1$ for some int. b

Example

Find 10^{-1} *rem 13*

$$a \cdot 10 \equiv 1 \pmod{13},$$
$$a \cdot 10 = 13 \cdot b + 1,$$

Listing multiples of both sides:

10, 20, 30, 40

14, 27, 40

So we have $4 \cdot 10 = 13 \cdot b + 1,$

$$4 \cdot 10 \equiv 1 \pmod{13},$$

and $10^{-1} = 4 \pmod{13}.$

Linear Congruences Modulo a Prime

Solve: $10x \equiv 2 \pmod{13}$

$10^{-1} \cdot 10x \equiv 2 \cdot 10^{-1} \pmod{13}$

$x \equiv 2 \cdot 10^{-1} \pmod{13}$

We know that $10^{-1} = 4 \pmod{13}$,

$x \equiv 2 \cdot 4 \pmod{13}$

$x \equiv 8 \pmod{13}$

Solve: $10x + 5 \equiv 2 \pmod{13}$

$10x + 13 \equiv 2 \pmod{13}$

$10x + 14 \equiv 2 \pmod{13}$

Modular systems of linear congruences

$$\begin{cases} x + 2y \equiv 7 \pmod 8 \\ 7y \equiv 7 \pmod 8 \end{cases}$$

Modular systems of linear congruences

$$\begin{cases} x + 2y \equiv 7 \pmod 8 \\ 7y \equiv 7 \pmod 8 \end{cases}$$

Solution: (5, 1).

Example

Let x be a positive integer, and $y = x^2 + 2$. Can x and y be both prime? The only tuple, for which it is possible is $x = 3$ and $y = 11$. Prove.

Assume that $x > 3$. (If $x = 1$, x is not prime; if $x = 2$, y is not prime.)
Depending on the remainder of x modulo 3, we have three cases:

1. $x \text{ (rem } 3) = 0$, then x is a multiple of 3, and so it is not prime;

2. $x \text{ (rem } 3) = 1$, then $y \text{ (rem } 3) = (x^2 + 2) \text{ (rem } 3) = (1^2 + 2) \text{ (rem } 3) = 0$, and y is not prime;
3. $x \text{ (rem } 3) = 2$, then $y \text{ (rem } 3) = (x^2 + 2) \text{ (rem } 3) = (2^2 + 2) \text{ (rem } 3) = 0$, and y is not prime.

In each of the three cases, either x, or y is not prime, and thus there is no tuple (x, y) for which both, x and y, are prime, except for $(3, 11)$.

Fermat's Little Theorem (FLT)

Pierre de Fermat

If *p* is a prime number, then for any integer *a*,

$$a^p \equiv a \pmod{p}$$

If *p* is a prime number, and *a* is not divisible by *p,* then

$$a^{p-1} \equiv 1 \pmod{p}$$

Fermat's Little Theorem

Proof (by Math Induction on a)

Base case: $1^p \equiv 1 \pmod p$ *is true.*
Suppose the statement $a^p \equiv a \pmod p$ *is true;*
need to prove that $(a+1)^p \equiv a+1 \pmod p$.

By binomial theorem,

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1$$

$\binom{p}{k} = \frac{p!}{k!(p-k)!}$, and since p is prime, $\binom{p}{k}$ *rem* $p \equiv 0$ for $1 \leq k \leq p-1$

Then $(a+1)^p \equiv a^p + 1 \pmod p$, *and using the assumption,*
$(a+1)^p \equiv a+1 \pmod p$.

Required !!!

Fermat's Little Theorem

Application

If p is a prime number, and a is not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Exponentiation :

Ex.1

$3^4 \text{ rem } 5 \equiv 1$

Ex. 2

$3^{17} \text{ rem } 5 \equiv 3^{4*4+1} \text{ rem } 5 \equiv (3^4)^4 \cdot 3 \text{ rem } 5 \equiv$

$1 \cdot 3 \text{ rem } 5 \equiv 3$

Fermat's Little Theorem

If p is a prime number, and a is not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Find an inverse using FLT

Ex. 3 Find 10^{-1} *rem 13.*

$10^{12} \equiv 1 \pmod{13}$ *(*from *FLT)*

Then $10^{-1} \text{ (rem 13)} \equiv 10^{-1} \cdot 10^{12} \text{ (rem 13)} \equiv$

$10^{11} \text{(rem 13)} \equiv \ldots$

Find 10^{-1} *(rem 7)*

Find 10^{-8} *(rem 13)*

Fermat's Last Theorem

No three positive integers *a, b*, and *c* can satisfy the equation

$$a^n + b^n = c^n$$

for any integer value of *n* greater than *2.*

Was stated by Pierre de Fermat in 1637, proved – by Andrew Wiles in 1994. Prior to its proof was in the Guinness Book of World Records for "most difficult mathematical proofs".

For n = 2, we have:

$$a^2 + b^2 = c^2$$

Such a set of three integers (a, b, c) is called a Pythagorean triple.

More Proofs

Prove or disprove:

$$\gcd(a^2, b^2) = (\gcd(a, b))^2$$

Prime Numbers

Theorem. There are infinitely many primes

Euclid's proof (by contradiction):

Suppose that $p_1=2 < p_2 = 3 < \ldots < p_r$ are all of the primes. Let $P = p_1p_2\ldots p_r+1$ and let p be a prime dividing P; then p can not be any of $p_1, p_2, \ldots, p_r$, otherwise p would divide the difference $P-p_1p_2\ldots p_r=1$, which is impossible. So this prime p is still another prime, and $p_1, p_2, \ldots, p_r$ would not be all of the primes.

Proof required for EC

Euler's Totient Function

Euler's totient function, $\phi(n)$ is an arithmetic function that counts the number of positive integers less than or equal to *n* that are relatively prime to *n*. Thus, if *n* is a positive integer ($n > 1$), then $\phi(n)$ is the number of integers *k* in the range $1 < k \leq n$ for which the greatest common divisor $\gcd(n, k) = 1$. $\phi(1) = 1$ by definition.

Euler's Totient Function

n	$\varphi(n)$	numbers coprime to n
1	1	1
2	1	1
3	2	1, 2
4	2	1,3
5	4	1,2,3,4
6	2	1,5
7	6	1,2,3,4,5,6
8	4	1,3,5,7
9	6	1,2,4,5,7,8
10	4	1,3,7,9
11	10	1,2,3,4,5,6,7,8,9,10
12	4	1,5,7,11
13	12	1,2,3,4,5,6,7,8,9,10,11,12
14	6	1,3,5,9,11,13
15	8	1,2,4,7,8,11,13,14

Euler's Totient Function

If p is prime:

$\varphi(p) = p - 1$

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$$

Let p be a prime number, and m some integer.

gcd(p^k, m) > 1 if $m = pl$ (for some int. l).

The multiples of p that are less than or equal to p^k are p, $2p$, $3p$, ..., p^k, and there are p^{k-1} of them.

Therefore the other $p^k - p^{k-1}$ numbers are all relatively prime to p^k.

Euler's Totient Function

$\varphi(n)$ is a multiplicative function:

if two numbers m and n are relatively prime (with respect to each other), then

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Euler's Totient Function

$$n = p_1^{k_1} \cdots p_r^{k_r}$$

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_r^{k_r}) \\
&= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) p_2^{k_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{k_r}\left(1 - \frac{1}{p_r}\right) \\
&= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).
\end{aligned}$$

$$\varphi(36) = \varphi\left(2^2 3^2\right) = 36\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12$$

Euler's Totient Theorem (generalization of FLT)

Theorem.

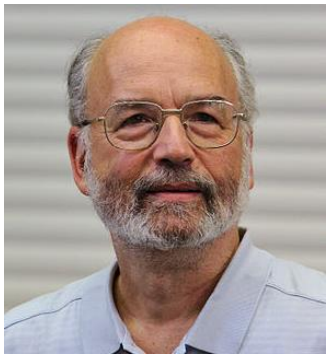
If ***a*** and ***n*** are relatively prime, then

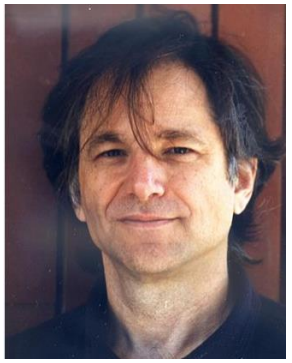
$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where φ(n) is Euler's totient function.

(The converse theorem is true as well.)

RSA (cryptosystem)



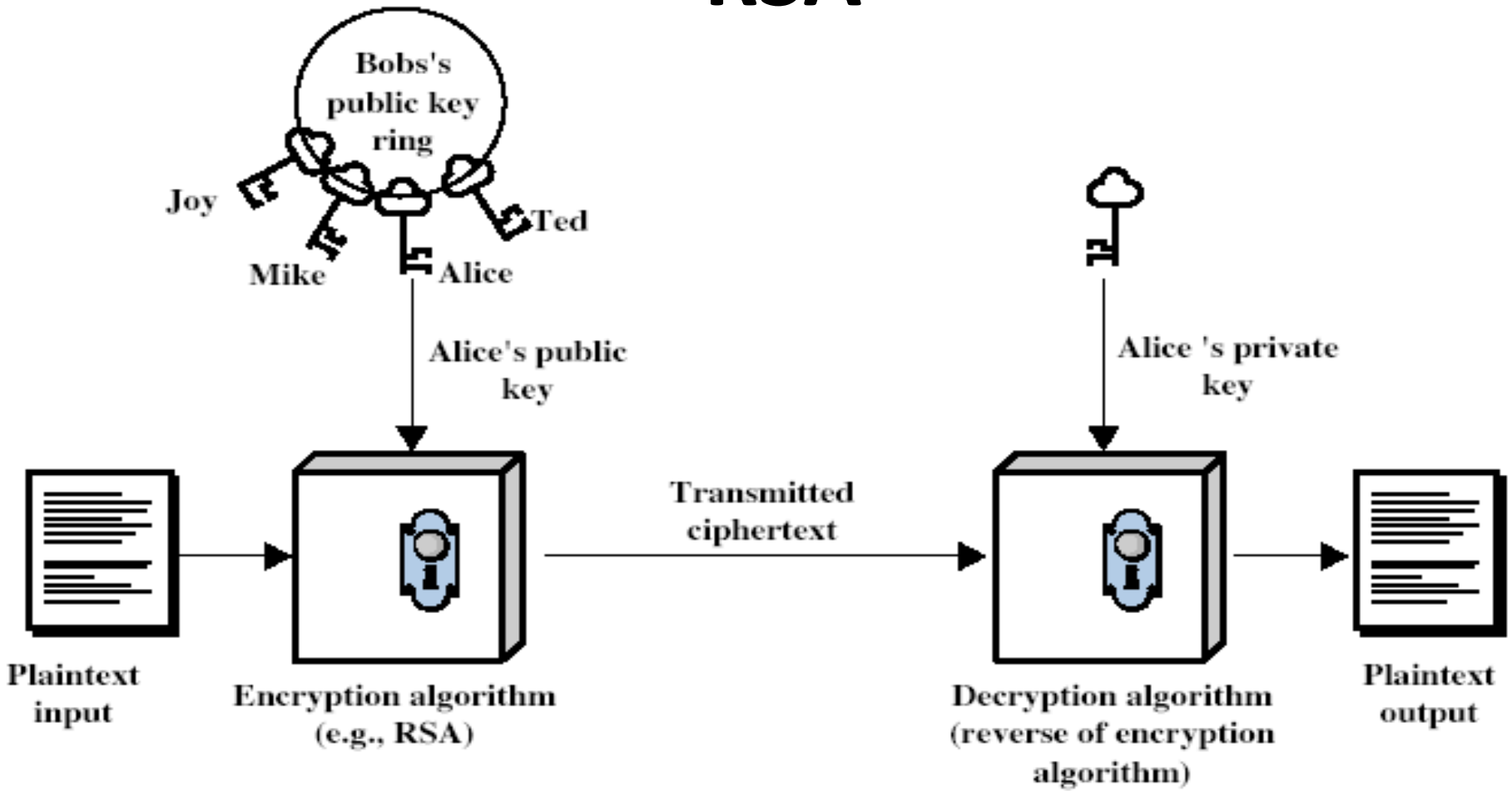


Ron **R**ivest Adi **S**hamir Leonard **A**dleman

The RSA algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT; the letters **RSA** are the initials of their surnames, listed in the same order as on the paper.

Used for secure data transmission.

RSA



William Stallings, Lawrie Brown

RSA

1. Generate two distinct primes, p and q. These are used to generate the private key, and they must be kept hidden. (In current practice, p and q are chosen to be hundreds of digits long.)
2. Let $n ::= pq$.
3. Select an integer $e \in [1, n)$ such that $\gcd(e, (p-1)(q-1)) = 1$. The *public key* is the pair (e, n). This should be distributed widely.
4. Compute $d \in [1, n)$ such that $de \equiv 1 \pmod{(p-1)(q-1)}$.

   The *private key* is the pair (d, n). This should be kept hidden!

RSA

Example:

Choose two distinct prime numbers p and q,

and let $n = pq$

$$p = 7;\ q = 13;\ \ n = 91;\ \ \varphi(n) = 6 \cdot 12 = 72;$$

Pick e (encryption exponent), s.t. $gcd(e, \varphi(n)) = 1$;

Public key: $P = (e, n)$

$$e = 5;\ \ gcd(5, 72) = 1;$$

Find d (decryption exponent), $d = e^{-1} \pmod{\varphi(n)};$

Secret key: $S = (d, n)$

$$d = 5^{-1} \pmod{72};$$

RSA

Example (cont.):

$5^{-1} \pmod{72}$ -- ?

$5 \cdot d \equiv 1 \pmod{72}$

5, 10, 15, 20, ..., 145

73, 145

$5 \cdot d = 145$

$d = 29$

Secret key: $S = (29, 91)$

RSA

a	b	c …	e = 5
|	|	|	d = 29
3	2	7	n = 91

Encrypting message ‘b’:

$$C = M^e \pmod{n}$$

M = 2: $C = 2^5 \pmod{91} = 32$

Decrypting message C:

$$M = C^d \pmod{n}$$

$$M = 32^{29} \pmod{91} = (32^2)^{14} \cdot 32 \pmod{91} = \ldots$$

$$= 2$$

RSA

What if ???

-- gcd(e, φ(n)) > 1;

$d \equiv e^{-1} \pmod{\varphi(n)}$;

$ed \equiv 1 \pmod{\varphi(n)}$;

If e = 4, mod φ(n) = 72; $4d \equiv 1 \pmod{72}$;

-- p and q are small

-- p = q *φ(n) = (p-1)(q-1) ?*

if p = q: *φ(n) = (p-1)(p-1) ???*

-- Is double inscription correct?

-- Is double inscription more secure?

RSA

What if ... ?

Problem 1: Below you are given five choices of parameters p, q, e, d of RSA. For each choice tell whether these parameters are correct[1] (write YES/NO). If the parameters are correct, compute the encryption of $M = 3$. If the parameters are incorrect, give a brief explanation why (at most 10 words).

p	q	e	d	correct?	Encrypt $M = 3$ if correct. Justify if not correct.
5	21	7	23		
13	7	5	29		
11	11	9	89		
7	17	11	37		
3	7	5	5		

RSA

What if ... ?

p	q	e	d	correct?	Encrypt $M = 3$ if correct. Justify if not correct.
5	21	7	23	NO	21 is not prime.
13	7	5	29	YES	Here $n = 91$. So $C = 3^5 = 61 \pmod{91}$.
11	11	9	89	NO	p and q cannot be equal.
7	17	11	37	NO	We have $\phi(n) = 96$, but $11 \cdot 37 = 407 = 23 \neq 1 \pmod{96}$.
3	7	5	5	YES	Here $n = 21$. So $C = 3^5 = 12 \pmod{21}$.

RSA

Correctness:

$$d^{-1} \equiv e \pmod{\varphi(n)}$$

$$ed \equiv 1 \pmod{\varphi(n)}$$

$$ed = 1 + k(p - 1)(q - 1)$$

$$M^{ed} = M^{1 + k(p - 1)(q - 1)} = M\,(M^{(p - 1)})^{k(q - 1)} \equiv M \pmod{p}$$

$$M^{ed} = M^{1 + k(p - 1)(q - 1)} = M\,(M^{(q - 1)})^{k(p - 1)} \equiv M \pmod{q}$$

and since p and q are prime,

$$M^{ed} \equiv M \pmod{pq}$$

Proof required for EC

Famous open and solved problems in number theory

Primality is easy!

A primality test is a test or algorithm for determining whether an input number is prime.

N is prime if it has no divisors less or equal to $\sqrt{N}$.

Prove, that all primes are of the form $6k \pm 1$.

Most popular algorithms for primality testing are probabilistic; may output a composite number as a prime.

Fermat's Primality Test

Fermat's little theorem: If *p* is a prime number, and *a* is not divisible by *p,* then

$$a^{p-1} \equiv 1 \pmod{p}$$

To test an integer *n* for primality:

Pick some integer **a**, s.t. $gcd(n, a) = 1;$

Check, whether $a^{n-1} \equiv 1 \pmod{n};$

If not, *n* is composite;

If yes, *n* is ???

Fermat's Primality Test, Carmichael numbers

If $a^{n-1} \equiv 1 \pmod{n}$, but n is not a prime number, it is called a (Fermat) pseudoprime base a;

The smallest pseudoprime base 2 is 341:

if n = 341 and a = 2, $2^{340} \equiv 1 \pmod{341}$,

but $341 = 11 \cdot 31$ and is composite.

A Carmichael number is a composite number n, which satisfies a congruence

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

for all a, s.t. $1 < a < n$, and $gcd(n, a) = 1$

The smallest Carmichael number is 561.

Miller-Rabin Primality Test

Let n (n > 2) be a prime number. Then n-1 is even.
Let $n - 1 = 2^s d$,
where s and d are positive integers, and d is odd.
For each a in $(\mathbf{Z}/n\mathbf{Z})^*$, either

$a^d \equiv 1 \pmod{n}$ (1), or

$a^{ld} \equiv -1 \pmod{n}$ (2),

(where $l = 2^r$ and $0 \leq r \leq s - 1$)

If we can find a, s.t. (1) and (2) are not true for all r, then n is not prime

Famous problems in number theory

The Prime Number Theorem

Let $\pi(x)$ be a function that counts the number of primes less than or equal to x. Then

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

among the positive integers of at most 1000 digits, about one in 2300 is prime;
among the positive integers of at most 2000 digits, about one in 4600 is prime;

Euler's theorem

If two integers *a* and *n* are relatively prime, then

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

where $\varphi(n)$ is Euler's totient function.

The converse is true as well.

Primality is easy, but Factoring is hard!

Factoring:

No efficient algorithm is known; ended in 2009: factoring a 232-digit number, utilizing hundreds of machines over a span of two years.

Famous problems in number theory

Fermat's Last Theorem

No three positive integers *a, b*, and *c* can satisfy the equation

$$a^n + b^n = c^n$$

for any integer value of *n* greater than *2.*
Was stated by Pierre de Fermat in 1637, proved – by Andrew Wiles in 1994. Prior to its proof was in the Guinness Book of World Records for “most difficult mathematical proofs”.

For n = 2, we have:

$$a^2 + b^2 = c^2$$

Such a set of three integers (a, b, c) is called a Pythagorean triple.

Famous problems in number theory

Goldbach's Conjecture

Every even integer greater than 2 can be expressed as the sum of two primes. (no proof!)

$4 = 2 + 2$ $6 = 3 + 3$ $8 = 3 + 5$

$50 = 3 + 47 = 7 + 43 = 13 + 37$

$100 = 3 + 97 = 11 + 89 = 17 + 83 = 29 + 71 = 41 + 59 = 47 + 53$

Has been shown to hold for all integers less than 4×10^{18}.

Goldbach's Conjecture

Goldbach's weak conjecture

Every odd number greater than 5 can be expressed as the sum of three primes. (A prime may be used more than once in the same sum.)

“Weak" since if Goldbach’s strong conjecture is proven, it would be true.

Was proved by Harald Helgott in 2013.

Famous problems in number theory

Twin Primes Conjecture

Twin primes are a pair of prime numbers of the form (p, p + 2).

There are infinitely many twin prime pairs. ?

As of today, the record twin prime pair is

$$3756801695685 \cdot 2^{666669} \pm 1$$

Theorem of Terence Tao and Ben Green

There are arbitary long arithmetic progression in the primes.

Examples :

$$(3, 5, 7) \quad (5, 11, 17) \quad (7, 13, 19)$$
$$(5, 11, 17, 23) \quad (7, 37, 67, 97, 127, 157)$$

$$\begin{aligned}(&156458812726904 3,\\ &156458812726904 3 + 27881031428250 0,\\ &156458812726904 3 + 2 \cdot 27881031428250 0, \ldots\\ &156458812726904 3 + 23 \cdot 27881031428250 0)\end{aligned}$$