Number Theory

Cryptography

School of Engineering and Technology
CQUniversity Australia

Prepared by Steven Gordon on 04 Jan 2022,
number.tex, r1963

Contents

Divides (definition)

b *divides* a if $a = mb$ for some m, where a, b and m are integers. We can also say b is a *divisor* of a, or $b|a$.

Divides (example)

3 divides 12, since $12 = 4 \times 3$. Also, 3 is a divisor of 12, or $3|12$.

Greatest Common Divisor (definition)

$\gcd(a, b)$ returns the greatest common divisor of integers a and b. There are efficient algorithms for finding the gcd, i.e. Euclidean algorithm.

Greatest Common Divisor (example)

$\gcd(12, 20) = 4$, since the divisors of 12 are (1, 2, 3, *4*, 6, 12) and the divisors of 20 are (1, 2, *4*, 5, 10, 20).

Relatively Prime (definition)

Two integers, a and b, are relatively prime if $\gcd(a, b) = 1$.

Relatively Prime (example)

$\gcd(7, 12) = 1$, since the divisors of 7 are (1, 7) and the divisors of 12 are (1, 2, 3, 4, 6, 12). Therefore 7 and 12 are relatively prime to each other.

Relatively Prime (exercise)

How many positive integers less than 10 are relatively prime with 10?

Prime Number (definition)

An integer $p > 1$ is a *prime number* if and only if its only divisors are $+1$, -1, $+p$ and $-p$.

Prime Number (example)

The divisors of 13 are (1, 13), that is, 1 and itself. Therefore 13 is a prime number. The divisors of 15 are (1, 3, 5, 15). Since the divisors include numbers other than 1 and itself, 15 is not prime.

First 300 Prime Numbers

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1-20	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
21-40	73	79	83	89	97	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173
41-60	179	181	191	193	197	199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
61-80	283	293	307	311	313	317	331	337	347	349	353	359	367	373	379	383	389	397	401	409
81-100	419	421	431	433	439	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541
101-120	547	557	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
121-140	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	769	773	787	797	809
141-160	811	821	823	827	829	839	853	857	859	863	877	881	883	887	907	911	919	929	937	941
161-180	947	953	967	971	977	983	991	997	1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
181-200	1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
201-220	1229	1231	1237	1249	1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
221-240	1381	1399	1409	1423	1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
241-260	1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
261-280	1663	1667	1669	1693	1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
281-300	1823	1831	1847	1861	1867	1871	1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987

Prime Factors (definition)

Any integer $a > 1$ can be factored as:

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$$

where $p_1 < p_2 < \ldots < p_t$ are prime numbers and where each a_i is a positive integer

Prime Factors (example)

The following are examples of integers expressed as prime factors:

$$13 = 13^1$$
$$15 = 3^1 \times 5^1$$
$$24 = 2^3 \times 3^1$$
$$50 = 2^1 \times 5^2$$
$$560 = 2^4 \times 5^1 \times 7^1$$
$$2800 = 2^4 \times 5^2 \times 7^1$$

Integers as Prime Factors (exercise)

Find the prime factors of 12870, 12936 and 30607.

Prime Factorization Problem (definition)

There are no known efficient, non-quantum algorithms that can find the prime factors of a sufficiently large number.

Prime Factorization Problem (example)

RSA Challenge involved researchers attempting to factor large numbers. Largest number measured in number of bits or decimal digits. Some records held over time are:

- 1991: 330 bits or 100 digits
- 2005: 640 bits or 193 digits
- 2009: 768 bits or 232 digits
- Equivalent of 2000 years on single core 2.2 GHz computer to factor 768 bit
- Current algorithms such as RSA rely on numbers of 1024, 2048 and even 4096 bits in length

Euler's Totient Function (definition)

Euler's totient function, $\phi(n)$, is the number of positive integers less than n and relatively prime to n. Also written as $\varphi(n)$ or $\text{Tot}(n)$.

Properties of Euler's Totient (definition)

Several useful properties of Euler's totient are:

$$\phi(1) = 1$$

For prime $p, \phi(p) = p - 1$

For primes p and $q, \phi(px \times q) = \phi(p) \times \phi(q) = (p-1) \times (q-1)$

Euler's Totient Function (example)

The integers relatively prime to 10, and less than 10, are: 1, 3, 7, 9. There are 4 such numbers. Therefore $\phi(10) = 4$.

The integers relatively prime to 11, and less than 11, are: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. There are 10 such numbers. Therefore $\phi(11) = 10$. The property could also be used since 11 is prime.

Since 7 is prime, $\phi(7) = 6$.

Since $77 = 7 \times 11$, then $\phi(77) = \phi(7 \times 11) = 6 \times 10 = 60$.

Contents

Modular arithmetic simple (definition)

Modular arithmetic is similar to normal arithmetic (addition, subtraction, multiplication, division) but the answers "wrap around".

mod operator (definition)

If a is an integer and n is a positive integer, then $a \bmod n$ is defined as the remainder when a is divided by n. n is called the *modulus*.

mod operator (example)

The following are several examples of mod:

$$3 \bmod 7 = 3, \text{ since } 0 \times 7 + 3 = 3$$

$$9 \bmod 7 = 2, \text{ since } 1 \times 7 + 2 = 9$$

$$10 \bmod 7 = 3, \text{ since } 1 \times 7 + 3 = 10$$

$$(-3) \bmod 7 = 4, \text{ since } (-1) \times 7 + 4 = -3$$

Congruent modulo (definition)

Two integers a and b are *congruent modulo* n if $(a \bmod n) = (b \bmod n)$. The congruence relation is written as:

$a \equiv b \pmod{n}$

When the modulus is known from the context, it may be written simply as a $\equiv b$.

Congruent modulo (example)

The following are examples of congruence:

$$3 \equiv 10 \pmod{7}$$

$$14 \equiv 4 \pmod{10}$$

$$3 \equiv 11 \pmod{8}$$

Modular arithmetic (definition)

Modular arithmetic with modulus n performs arithmetic operations within the confines of set $Z_n = \{0, 1, 2, \ldots, (n-1)\}$.

mod in Z_7 (example)

Consider the set:

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

All modular arithmetic operations in mod 7 return answers in Z_7.

Modular Arithmetic

- If a is an integer and n is a positive integer, we define $a \bmod n$ to be the remainder when a is divided by n
- n is called the *modulus*
- Two integers a and b are *congruent modulo* n if $(a \bmod n) = (b \bmod n)$, which is written as

$$a \equiv b \pmod{n}$$

- $\pmod{n}$ operator maps all integers into the set of integers $Z_n = \{0, 1, \ldots, (n-1)\}$
- *Modular arithmetic* performs arithmetic operations within confines of set Z_n

Modular Addition (definition)

Addition in mod n is performed as normal addition, with the answer then mod by n.

Modular Addition (example)

The following are several examples of modular addition:

$$2 + 3 \pmod 7 = 5 \pmod 7 = 5 \bmod 7 = 5 \pmod 7$$

$$2 + 6 \pmod 7 = 8 \pmod 7 = 8 \bmod 7 = 1 \pmod 7$$

$$6 + 6 \pmod 7 = 12 \pmod 7 = 12 \bmod 7 = 5 \pmod 7$$

$$3 + 4 \pmod 7 = 7 \pmod 7 = 7 \bmod 7 = 0 \pmod 7$$

Additive Inverse (definition)

a is the *additive inverse* of b in mod n, if $a + b \equiv 0 \pmod{n}$.

For brevity, AI(a) may be used to indicate the additive inverse of a. One property is that all integers have an additive inverse.

Additive Inverse (example)

In mod 7:

$$AI(3) = 4, \text{ since } 3 + 4 \equiv 0 \pmod{7}$$

$$AI(6) = 1, \text{ since } 6 + 1 \equiv 0 \pmod{7}$$

In mod 12:

$$AI(3) = 9, \text{ since } 3 + 9 \equiv 0 \pmod{12}$$

Modular Subtraction (definition)

Subtraction in mod n is performed by addition of the additive inverse of the subtracted operand. This is effectively the same as normal subtraction, with the answer then mod by n.

Modular Subtraction (example)

For brevity, the modulus is sometimes omitted and $=$ is used in replace of $\equiv$. In mod 7:

$$6 - 3 = 6 + \mathrm{AI}(3) = 6 + 4 = 10 = 3 \pmod 7$$

$$6 - 1 = 6 + \mathrm{AI}(1) = 6 + 6 = 12 = 5 \pmod 7$$

$$1 - 3 = 1 + \mathrm{AI}(3) = 1 + 4 = 5 \pmod 7$$

While the first two examples obviously give answers as we expect from normal subtraction, the third does as well. $1 - 3 = -2$, and in mod 7, $-2 \equiv 5$ since $-1 \times 7 + 5 = (-2)$. Recall $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

Modular Multiplication (definition)

Modular multiplication is performed as normal multiplication, with the answer then mod by n.

Modular Multiplication (example)

In mod 7:

$$2 \times 3 = 6 \pmod 7$$

$$2 \times 6 = 12 = 5 \pmod 7$$

$$3 \times 4 = 12 = 5 \pmod 7$$

Multiplicative Inverse (definition)

a is a multiplicative inverse of b in mod n if $a \times b \equiv 1 \pmod{n}$. For brevity, MI($a$) may be used to indicate the multiplicative inverse of a. a has a multiplicative inverse in $(\text{mod } n)$ if a is relatively prime to n.

Multiplicative Inverse in mod 7 (example)

2 and 7 are relatively prime, therefore 2 has a multiplicative inverse in mod 7.

$$2 \times 4 \pmod 7 = 1, \text{ therefore } MI(2) = 4 \text{ and } MI(4) = 2$$

3 and 7 are relatively prime, therefore 3 has a multiplicative inverse in mod 7.

$$3 \times 5 \pmod 7 = 1, \text{ therefore } MI(3) = 5 \text{ and } MI(5) = 3$$

$\phi(7) = 6$, meaning 1, 2, 3, 4, 5 and 6 are relatively prime with 7, and therefore all of those numbers have a MI in mod 7.

Multiplicative Inverse in mod 8 (example)

3 and 8 are relatively prime, therefore 3 has a multiplicative inverse in mod 8.

$$3 \times 3 \pmod 8 = 1, \text{ therefore } MI(3) = 3$$

4 and 8 are NOT relatively prime, therefore 4 does not have a multiplicative inverse in mod 8. $\phi(8) = 4$, and therefore only 4 numbers (1, 3, 5, 7) have a MI in mod 8.

Modular Division (definition)

Division in mod n is performed as modular multiplication of the multiplicative inverse of 2nd operand. Modular division is only possible when the 2nd operand has a multiplicative inverse, otherwise the operation is undefined.

Modular Division (example)

In mod 7:

$$5 \div 2 = 5 \times MI(2) = 5 \times 4 = 20 \equiv 6$$

In mod 8:

$$7 \div 3 = 7 \times MI(3) = 7 \times 3 = 21 \equiv 5$$

$7 \div 4$ is undefined, since 4 does not have a multiplicative inverse in mod 8.

Properties of Modular Arithmetic (definition)

$$(a \bmod n) \bmod n = a \bmod n$$

$$[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$$

$$[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$$

$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

Commutative, associative and distributive laws similar to normal arithmetic also hold.

Contents

Fermat's Theorem 1 (definition)

If p is prime and a is a positive integer not divisible by p, then:

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

Fermat's Theorem 2 (definition)

If p is prime and a is a positive integer, then:

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

There are two forms of Fermat's theorem—use whichever form is most convenient.

Fermat's theorem (example)

What is $27^{42} \bmod 43$? Since 43 is prime and $42 = 43 - 1$, this matches Fermat's Theorem form 1. Therefore the answer is 1.

Fermat's theorem (example)

What is $640^{163} \bmod 163$? Since 163 is prime, this matches Fermat's Theorem form 2. Therefore the answer is 640, or simplified to $640 \bmod 163 = 151$.

Euler's Theorem 1 (definition)

For every a and n that are relatively prime:

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

Euler's Theorem 2 (definition)

For positive integers a and n:

$$a^{\phi(n)+1} \equiv a \pmod{n}$$

Note that there are two forms of Euler's theorem—use the most relevant form.

Euler's theorem (example)

Show that $37^{40} \bmod 41 = 1$. Since $n = 41$, which is prime, then $\phi(41) = 40$. As 37 is also prime, 37 and 41 are relatively prime. Therefore Euler's Theorem form 1 holds.

Euler's theorem (example)

What is $13794^{4621} \bmod 4757$? Factoring 4757 into primes gives 67×71. Therefore $\phi(4757) = \phi(67)x \times \phi(71) = 66 \times 70 = 4620$. Therefore, this follows Euler's Theorem form 2, giving an answer of 13794.

Contents

Modular Exponentiation (definition)

As exponentiation is just repeated multiplication, modular exponentiation is performed as normal exponentiation with the answer mod by n.

Modular Exponentiation (example)

$$2^3 \bmod 7 = 8 \bmod 7 = 1$$

$$3^4 \bmod 7 = 81 \bmod 7 = 4$$

$$3^6 \bmod 8 = 729 \bmod 8 = 1$$

Normal Logarithm (definition)

If $b = a^i$, then:

$$i = \log_a(b)$$

read as "the log in base a of b is index (or exponent) i".

The above definition is for normal arithmetic, not for modular arithmetic. Logarithm in normal arithmetic is the inverse operation of exponentiation. In modular arithmetic, modular logarithm is more commonly called *discrete logarithm*. Note we replace n with p—the reason will become apparent shortly.

Discrete Logarithm (definition)

If $b = a^i \pmod{p}$, then:

$$i = \mathrm{dlog}_{a,p}(b)$$

A unique exponent i can be found if a is a *primitive root* of the prime p.

Primitive Root (definition)

If a is a primitive root of prime p then $a_1, a_2, a_3, \ldots a_{p-1}$ are distinct in mod p.

The integers with a primitive root are: 2, 4, p^α, $2p^\alpha$ where p is any odd prime and α is a positive integer.

Primitive Root (example)

Consider the prime $p = 7$:
$a = 1 : 1^2 \bmod 7 = 1, 1^3 \bmod 7 = 1, \ldots$(not distinct)
$a = 2 : 2^2 \bmod 7 = 4, 2^3 \bmod 7 = 1, 2^4 \bmod 7 = 2, 2^5 \bmod 7 = 4, \ldots$(not distinct)
$a = 3 : 3^2 \bmod 7 = 2, 3^3 \bmod 7 = 6, 3^4 \bmod 7 = 4, 3^5 \bmod 7 = 5, 3^6 \bmod 7 = 1$(distinct)
Therefore 3 is a primitive root of 7 (but 1 and 2 are not).

Powers of Integers, modulo 7

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

From the above table we see 3 and 5 are primitive roots of 7.

Discrete Logs, modulo 7

Discrete Logarithms to the base 3, modulo 7

a	**1**	**2**	**3**	**4**	**5**	**6**
$dlog_{3,7}(a)$	6	2	1	4	5	3

Discrete Logarithms to the base 5, modulo 7

a	**1**	**2**	**3**	**4**	**5**	**6**
$dlog_{5,7}(a)$	6	4	5	2	1	3

Discrete logarithms to the base 3, modulo 7 are distinct since 3 is a primitive root of 7. Discrete logarithms to the base 5, modulo 7 are distinct since 5 is a primitive root of 7.

Powers of Integers, modulo 17

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1
3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1
5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1
9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1
10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1

We see that 3, 5, 6, 7, 10, 11, 12 and 14 are primitive roots of 17.

Discrete Logarithms, modulo 17

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{dlog}_{3,17}(a)$	16	14	1	12	5	15	11	10	2	3	7	13	4	5	14	8

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{dlog}_{5,17}(a)$	16	6	13	12	1	3	15	2	10	7	11	9	4	5	14	8

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{dlog}_{6,17}(a)$	16	2	15	4	11	1	5	6	14	13	9	3	12	7	10	8

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{dlog}_{7,17}(a)$	16	10	3	4	15	13	1	14	6	9	5	7	12	11	2	8

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{dlog}_{10,17}(a)$	16	10	11	4	7	5	9	14	6	1	13	15	12	3	2	8

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{dlog}_{11,17}(a)$	16	2	7	4	3	9	13	6	14	5	1	11	12	15	10	8

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{dlog}_{12,17}(a)$	16	6	5	12	9	11	7	2	10	15	3	1	4	13	14	8

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{dlog}_{14,17}(a)$	16	14	9	12	13	7	3	10	2	11	15	5	4	1	6	8

The discrete logarithm in modulo 17 can be calculated for the 8 primitive roots.

Contents

Hard Problem: Integer Factorisation (definition)

If p and q are unknown primes, given $n = pq$, find p and q.

Also known as prime factorisation. While someone that knows p and q can easily calculate n, if an attacker knows only n they cannot find p and q.

Hard Problem: Euler's Totient (definition)

Given composite n, find $\phi(n)$.

While it is easy to calculate Euler's totient of a prime, or of the multiplication of two primes if those primes are known, an attacker cannot calculate Euler's totient of sufficiently large non-prime number. Solving Euler's totient of n, where $n = pq$, is considered to be harder than integer factorisation.

Hard Problem: Discrete Logarithms (definition)

Given b, a, and p, find i such that $i = \text{dlog}_{a,p}(b)$.

While modular exponentiation is relatively easy, such as calculating $b = a^i \bmod p$, the inverse operation of discrete logarithms is computationally hard. The complexity is considered comparable to that of integer factorisation.

When studying RSA and Diffie-Hellman, you will see how these hard problems in number theory are used to secure ciphers.