Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Number Theory

Cryptography

School of Engineering and Technology CQUniversity Australia

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

◆□ > ◆□ > ◆ □ > ● □ > ◆ □ > ● □ >

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Contents

### **Divisibility and Primes**

Modular Arithmetic

Fermat's and Euler's Theorems

**Discrete Logarithms** 

Computationally Hard Problems

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# 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.

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# Divides (example)

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

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### 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.

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### 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).

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# Relatively Prime (definition)

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# 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.

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# Relatively Prime (exercise)

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

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# Prime Number (definition)

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

## 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.

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### First 300 Prime Numbers

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863	877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
	1           2           73           179           283           419           547           661           947           1087           1381           1523           1663           1663	1         2           2         3           73         79           179         181           283         293           419         421           547         557           661         673           911         213           101         213           112         101           123         131           134         139           155         151           164         164           155         165           164         164           155         165           165         165           165         165           165         165	2         3         3           2         3         5           73         79         83           179         181         191           283         293         307           410         421         313           547         557         563           616         673         677           811         821         823           947         953         967           1010         1011         1019           1223         1231         1232           1341         1349         1349           1424         1341         1349           1525         1234         1349           1526         1241         1349           1527         1349         1349           1528         1351         1349           1529         1351         1349           1529         1351         1349           1539         1351         1349           1549         1354         1349	2         3         3         4           2         3         5         7           73         79         83         89           179         181         191         193           283         293         307         311           419         421         431         433           547         557         563         563           618         673         874         833           619         577         563         563           610         673         674         833           611         623         677         563           612         673         674         833           613         624         627         573           614         623         627         573           615         624         627         573           616         1021         623         574           617         624         624         574           618         1029         1231         1243           619         1249         1243         1243           619         1249         1244         1244	2         3         4         5           2         3         5         7         11           73         79         83         89         97           179         181         193         197         193           283         293         301         313         313           419         421         431         433         439           547         557         563         569         511           641         673         674         673         674         614           642         673         674         673         674         614           643         674         675         683         671         615           644         673         674         673         674         674           645         674         675         674         674         674           647         673         674         674         674         674           647         674         674         674         674         674           648         649         649         649         649         649           649         649	2         3         4         5         6           2         3         5         7         11         13           73         79         83         89         97         101           170         181         191         193         197         181           170         181         191         133         197         181           181         191         131         133         137           182         293         607         313         133         137           193         421         431         433         433         433           547         557         563         564         571         577           641         673         677         683         691         571           547         557         563         567         571         571           643         673         673         674         673         571           544         675         675         571         571         571           545         675         574         573         571         571           546         1637         1637	2         3         4         5         6         7           2         3         5         7         11         13         17           73         7         8         9         9         101         103           17         18         19         9         9         101         103           17         18         19         19         17         103         11           18         191         13         13         13         131           193         293         307         11         313         314         313           194         421         431         433         433         433         314         314           194         421         431         433         433         434         434           547         557         563         569         571         577         587           547         573         563         563         564         574         574         574           547         574         575         575         574         574         574         574           549         575         575         <	2         3         4         5         6         7         8           2         3         5         7         11         13         17         17           73         79         83         89         97         101         103         107           170         181         191         193         197         101         103         107           170         181         191         193         197         101         103         101           181         191         193         197         193         1311         131         131         131 </th <th>2         3         4         5         6         7         8         9           2         3         5         7         11         13         17         19         23           73         79         83         80         97         101         103         107         103           173         79         83         89         97         101         103         107         203           174         181         191         193         197         210         223         277           283         293         607         314         133         417         313         317         313           420         293         607         314         433         439         439         437         437           543         623         626         571         577         587         593</th> <th>2         3         4         5         6         7         8         9         10           2         3         5         7         11         13         17         10         23         23           73         79         33         89         97         10         13         17         10         13         10         13         13           170         181         193         193         107         103         101         103         103         131           170         181         193         193         193         131         131         131         133         131         133         131         133         131         133         131         133         131         133         131         133         131         133         131         133         1311         131         131</th> <th>12345678910112357111317192329317379838997103107103107103107103107101313137131131131131233233233233233203203203303314313314314313314315314315314403421431433439434449457464463467547557563569571576573574575563563563643673673674673674674675676676676643674675676676676676676676676676644674675676676676676676676676676676645674676676676676676676676676676676676646676676676676676676676676676676676676647676676676676676676676676676676676676676676676676676676&lt;</th> <th>2         3         4         5         6         7         8         9         10         11         12           2         3         5         7         11         13         17         19         23         29         31         37           73         79         83         89         97         101         103         107         109         123         124         137           173         79         83         89         97         101         103         107         108         124         124         131           170         181         191         193         197         131         132         127         220         231         233         235           181         191         193         191         131         <t< th=""><th>1         2         3         4         5         6         7         8         9         10         11         12           2         3         5         7         11         13         17         10         23         20         31         37         41           73         79         83         89         97         10         103         107         103         13         13         137           170         181         193         197         101         103         107         103         13         137         131         133         137           181         193         193         193         131         133         137         131         133         137         131         133         137         131         133         137         131         133         137         131         <td< th=""><th>123456789101112132357111317192329313741377983899710110310710910310710110710110110110101102103103101101101101101101101101101101103104103104104104104104104104101101101104105105105105105105105105101101101101101105105105105105105105105105105101101101101101101101106107106107106107106107106105106101<!--</th--><th>1234567891011121314152355711131719232321313143437379838997101103107109101107101107101107101107101107101107101</th></th></td<><th>123456789101112131415162357111317102329303731434733377083807010&lt;</th><th>12345678910111213141416162357111112121223233131414343434337783809710<!--</th--><th>12345678910101213141516171823571111171720203137<td< th=""><th>123456789101112131414161718192357111317102329203137414347535051573783806010103101010310103<td< th=""></td<></th></td<></th></th></th></t<></th>	2         3         4         5         6         7         8         9           2         3         5         7         11         13         17         19         23           73         79         83         80         97         101         103         107         103           173         79         83         89         97         101         103         107         203           174         181         191         193         197         210         223         277           283         293         607         314         133         417         313         317         313           420         293         607         314         433         439         439         437         437           543         623         626         571         577         587         593	2         3         4         5         6         7         8         9         10           2         3         5         7         11         13         17         10         23         23           73         79         33         89         97         10         13         17         10         13         10         13         13           170         181         193         193         107         103         101         103         103         131           170         181         193         193         193         131         131         131         133         131         133         131         133         131         133         131         133         131         133         131         133         131         133         131         133         1311         131         131	12345678910112357111317192329317379838997103107103107103107103107101313137131131131131233233233233233203203203303314313314314313314315314315314403421431433439434449457464463467547557563569571576573574575563563563643673673674673674674675676676676643674675676676676676676676676676644674675676676676676676676676676676645674676676676676676676676676676676676646676676676676676676676676676676676676647676676676676676676676676676676676676676676676676676676<	2         3         4         5         6         7         8         9         10         11         12           2         3         5         7         11         13         17         19         23         29         31         37           73         79         83         89         97         101         103         107         109         123         124         137           173         79         83         89         97         101         103         107         108         124         124         131           170         181         191         193         197         131         132         127         220         231         233         235           181         191         193         191         131 <t< th=""><th>1         2         3         4         5         6         7         8         9         10         11         12           2         3         5         7         11         13         17         10         23         20         31         37         41           73         79         83         89         97         10         103         107         103         13         13         137           170         181         193         197         101         103         107         103         13         137         131         133         137           181         193         193         193         131         133         137         131         133         137         131         133         137         131         133         137         131         133         137         131         <td< th=""><th>123456789101112132357111317192329313741377983899710110310710910310710110710110110110101102103103101101101101101101101101101101103104103104104104104104104104101101101104105105105105105105105105101101101101101105105105105105105105105105105101101101101101101101106107106107106107106107106105106101<!--</th--><th>1234567891011121314152355711131719232321313143437379838997101103107109101107101107101107101107101107101107101</th></th></td<><th>123456789101112131415162357111317102329303731434733377083807010&lt;</th><th>12345678910111213141416162357111112121223233131414343434337783809710<!--</th--><th>12345678910101213141516171823571111171720203137<td< th=""><th>123456789101112131414161718192357111317102329203137414347535051573783806010103101010310103<td< th=""></td<></th></td<></th></th></th></t<>	1         2         3         4         5         6         7         8         9         10         11         12           2         3         5         7         11         13         17         10         23         20         31         37         41           73         79         83         89         97         10         103         107         103         13         13         137           170         181         193         197         101         103         107         103         13         137         131         133         137           181         193         193         193         131         133         137         131         133         137         131         133         137         131         133         137         131         133         137         131 <td< th=""><th>123456789101112132357111317192329313741377983899710110310710910310710110710110110110101102103103101101101101101101101101101101103104103104104104104104104104101101101104105105105105105105105105101101101101101105105105105105105105105105105101101101101101101101106107106107106107106107106105106101<!--</th--><th>1234567891011121314152355711131719232321313143437379838997101103107109101107101107101107101107101107101107101</th></th></td<> <th>123456789101112131415162357111317102329303731434733377083807010&lt;</th> <th>12345678910111213141416162357111112121223233131414343434337783809710<!--</th--><th>12345678910101213141516171823571111171720203137<td< th=""><th>123456789101112131414161718192357111317102329203137414347535051573783806010103101010310103<td< th=""></td<></th></td<></th></th>	123456789101112132357111317192329313741377983899710110310710910310710110710110110110101102103103101101101101101101101101101101103104103104104104104104104104101101101104105105105105105105105105101101101101101105105105105105105105105105105101101101101101101101106107106107106107106107106105106101 </th <th>1234567891011121314152355711131719232321313143437379838997101103107109101107101107101107101107101107101107101</th>	1234567891011121314152355711131719232321313143437379838997101103107109101107101107101107101107101107101107101	123456789101112131415162357111317102329303731434733377083807010<	12345678910111213141416162357111112121223233131414343434337783809710 </th <th>12345678910101213141516171823571111171720203137<td< th=""><th>123456789101112131414161718192357111317102329203137414347535051573783806010103101010310103<td< th=""></td<></th></td<></th>	12345678910101213141516171823571111171720203137 <td< th=""><th>123456789101112131414161718192357111317102329203137414347535051573783806010103101010310103<td< th=""></td<></th></td<>	123456789101112131414161718192357111317102329203137414347535051573783806010103101010310103 <td< th=""></td<>

Credit: Wikipedia, https://en.wikipedia.org/wiki/List\_of\_prime\_numbers, CC BY-SA 3.0

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

# 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

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# Prime Factors (example)

The following are examples of integers expressed as prime factors:

$$13 = 13^{1}$$

$$15 = 3^{1} \times 5^{1}$$

$$24 = 2^{3} \times 3^{1}$$

$$50 = 2^{1} \times 5^{2}$$

$$560 = 2^{4} \times 5^{1} \times 7^{1}$$

$$2800 = 2^{4} \times 5^{2} \times 7^{1}$$

・ロト ・日・・日・・日・・ つくぐ

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Integers as Prime Factors (exercise)

Find the prime factors of 12870, 12936 and 30607.

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Prime Factorization Problem (definition)

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### 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

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### 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 Tot(n).

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### 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,  $\phi(px \times q) = \phi(p) \times \phi(q) = (p-1) \times (q-1)$ 

Number Theory

#### Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

## 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  $\phi(77) = \phi(7 \times 11) = 6 \times 10 = 60$ .

Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Contents

Divisibility and Primes

### Modular Arithmetic

Fermat's and Euler's Theorems

**Discrete Logarithms** 

Computationally Hard Problems

### Cryptography Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

## Modular arithmetic simple (definition)

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

Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# mod operator (definition)

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

Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# mod operator (example)

The following are several examples of mod:

3 mod 7 = 3, since 
$$0 \times 7 + 3 = 3$$

9 mod 7 = 2, since  $1 \times 7 + 2 = 9$ 

10 mod 7 = 3, since  $1 \times 7 + 3 = 10$ 

 $(-3) \mod 7 = 4$ , since  $(-1) \times 7 + 4 = -3$ 

Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

## Congruent modulo (definition)

Two integers *a* and *b* are *congruent modulo n* if  $(a \mod n) = (b \mod n)$ . 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  $\equiv b$ .

Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# Congruent modulo (example)

The following are examples of congruence:

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

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

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Modular arithmetic (definition)

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

# 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  $Z_7$ .

Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Modular Arithmetic

- If a is an integer and n is a positive integer, we define a mod 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 mod n) = (b mod n), which is written as

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

- ▶ (mod n) operator maps all integers into the set of integers Z<sub>n</sub> = {0,1,...,(n-1)}
- Modular arithmetic performs arithmetic operations within confines of set  $Z_n$

Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Modular Addition (definition)

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

Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# Modular Addition (example)

The following are several examples of modular addition:

$$2+3 \pmod{7} = 5 \pmod{7} = 5 \pmod{7} = 5 \pmod{7} = 5 \pmod{7}$$

$$2+6 \pmod{7} = 8 \pmod{7} = 8 \mod{7} = 1 \pmod{7}$$

$$6+6 \pmod{7} = 12 \pmod{7} = 12 \pmod{7} = 5 \pmod{7}$$

$$3+4 \pmod{7} = 7 \pmod{7} = 7 \pmod{7} = 0 \pmod{7}$$

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### 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.

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# Additive Inverse (example)

In mod 7:

$$AI(3) = 4$$
, since  $3 + 4 \equiv 0 \pmod{7}$   
 $AI(6) = 1$ , since  $6 + 1 \equiv 0 \pmod{7}$ 

### In mod 12:

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

◆□ > ◆□ > ◆三 > ◆三 > ・三 · のへで

### Cryptography Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

## 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.

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Modular Subtraction (example)

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

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

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

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

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

Cryptography Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Modular Multiplication (definition)

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

Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

## Modular Multiplication (example)

In mod 7:

- $2 \times 3 = 6 \pmod{7}$  $2 \times 6 = 12 = 5 \pmod{7}$
- $3\times 4=12=5\pmod{7}$

### Cryptography Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### 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 (mod *n*) if *a* is relatively prime to *n*.

Cryptography Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Multiplicative Inverse in mod 7 (example)

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

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

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

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Multiplicative Inverse in mod 8 (example)

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

 $3 \times 3 \pmod{8} = 1$ , 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.

▲□▶▲□▶▲□▶▲□▶ □ の00

### Cryptography Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### 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.

Number Theory

Divisibility and Primes

#### Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

# Modular Division (example)

In mod 7:

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

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.

#### Cryptography Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Properties of Modular Arithmetic (definition)

 $(a \mod n) \mod n = a \mod n$  $[(a \mod n) + (b \mod n)] \mod n = (a + b) \mod n$  $[(a \mod n) - (b \mod n)] \mod n = (a - b) \mod n$  $[(a \mod n) \times (b \mod n)] \mod n = (a \times b) \mod n$ 

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Contents

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

**Discrete Logarithms** 

Computationally Hard Problems

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Fermat's Theorem 1 (definition)

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

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Fermat's Theorem 2 (definition)

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

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

▲□▶ ▲□▶ ▲三▶ ▲三▶ 三三 - のへの

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Fermat's theorem (example)

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Fermat's theorem (example)

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

# Euler's Theorem 1 (definition)

For every a and n that are relatively prime:

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

### Euler's Theorem 2 (definition)

For positive integers *a* and *n*:

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

## Euler's theorem (example)

Show that  $37^{40} \mod 41 = 1$ . 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.

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

## Euler's theorem (example)

What is 13794<sup>4621</sup> mod 4757? Factoring 4757 into primes gives  $67 \times 71$ . 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.

#### Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Contents

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

## Modular Exponentiation (definition)

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

#### Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

## Modular Exponentiation (example)

- $2^3 \mod 7 = 8 \mod 7 = 1$
- $3^4 \mod 7 = 81 \mod 7 = 4$
- $3^6 \bmod 8 = 729 \bmod 8 = 1$

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

# 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".

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

# Discrete Logarithm (definition)

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

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

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

Discrete Logarithms

Computationally Hard Problems

# 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,  $p^{\alpha}$ ,  $2p^{\alpha}$  where p is any odd prime and  $\alpha$  is a positive integer.

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

## Primitive Root (example)

Consider the prime p = 7:  $a = 1 : 1^2 \mod 7 = 1, 1^3 \mod 7 = 1, ... (\text{not distinct})$   $a = 2 : 2^2 \mod 7 = 4, 2^3 \mod 7 = 1, 2^4 \mod 7 = 2, 2^5 \mod 7 = 4, ... (\text{not distinct})$  $a = 3 : 3^2 \mod 7 = 2, 3^3 \mod 7 = 6, 3^4 \mod 7 = 4, 3^5 \mod 7 = 5, 3^6 \mod 7 = 1 (\text{distinct})$ 

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

Therefore 3 is a primitive root of 7 (but 1 and 2 are not).

#### Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Powers of Integers, modulo 7

a	a <sup>2</sup>	a <sup>3</sup>	a <sup>4</sup>	a <sup>5</sup>	a <sup>6</sup>
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

#### Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Discrete Logs, modulo 7

Discrete Logarithms to the base 3, modulo 7

a	1	2	3	4	5	6
dlog <sub>3,7</sub> (a)	6	2	1	4	5	3

### Discrete Logarithms to the base 5, modulo 7

a	1	2	3	4	5	6
dlog <sub>5,7</sub> (a)	6	4	5	2	1	3

#### Number Theory

Discrete Logarithms

Ρ	owe	rs o	f Int	ege	rs, n	nodi	ulo :	17							
	a	<b>a</b> <sup>2</sup>	<b>a</b> 3	a4	a <sup>5</sup>	<b>a</b> 6	a7	ഷ	a9	<b>a</b> 10	a11	a <sup>12</sup>	a13	a14	
	1	4	1	1	1	1	1	1	1	1	1	1	1	1	
	1	1	1	1	1	1	1	1	1	T	T	T	T	T	
	2	4	8	16	15	13	9	1	2	4	8	16	15	13	
	3	9	10	13	5	15	11	16	14	8	7	4	12	2	
	4	16	13	1	4	16	13	1	4	16	13	1	4	16	
	5	8	6	13	14	2	10	16	12	9	11	4	3	15	
	6	2	12	4	7	8	14	16	11	15	5	13	10	9	Ī
	7	15	3	4	11	9	12	16	10	2	14	13	6	8	
	8	13	2	16	9	4	15	1	8	13	2	16	9	4	
	9	13	15	16	8	4	2	1	9	13	15	16	8	4	
	10	15	14	4	6	9	5	16	7	2	3	13	11	8	
	11	2	5	4	10	8	3	16	6	15	12	13	7	9	Ī
	12	8	11	13	3	2	7	16	5	9	6	4	14	15	Ī
	13	16	4	1	13	16	4	1	13	16	4	1	13	16	Î
	14	9	7	13	12	15	6	16	3	8	10	4	5	2	Ī

a15

 $a^{16}$ 

#### Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Discrete Logarithms, modulo 17

а	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$dlog_{3,17}(a)$	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
dlog <sub>5,17</sub> (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
$dlog_{6,17}(a)$	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
dlog <sub>7,17</sub> (a)	16	10	3	4	15	13	1	14	6	9	5	7	12	11	2	8
а	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
dlog <sub>10,17</sub> (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
dlog <sub>11,17</sub> (a)	16	2	7	4	3	9	13	6	14	5	1	11	12	15	10	8
а	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
dlog <sub>12,17</sub> (a)	16	6	5	12	9	11	7	2	10	15	3	1	4	13	14	8
а	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
dlog <sub>14,17</sub> (a)	16	14	9	12	13	7	3	10	2	11	15	5	4	1	6	8

▲□▶ ▲圖▶ ▲≣▶ ▲≣▶ = ■ - のへで

#### Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Contents

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorems

**Discrete Logarithms** 

Computationally Hard Problems

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Hard Problem: Integer Factorisation (definition)

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Hard Problem: Euler's Totient (definition)

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

Number Theory

Divisibility and Primes

Modular Arithmetic

Fermat's and Euler's Theorem

Discrete Logarithms

Computationally Hard Problems

### Hard Problem: Discrete Logarithms (definition)

Given b, a, and p, find i such that  $i = dlog_{a,p}(b)$ .