Prime Numbers

- Prime numbers only have divisors of 1 and itself
  - They cannot be written as a product of other numbers

- Prime numbers are central to number theory

- Any integer a > 1 can be factored in a unique way as

$$a = {}_{p1}{}^{a1} * p_2{}^{a2} * . . . * p_{p1}{}^{a1}$$

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

- This is known as the fundamental theorem of arithmetic

Number Theory

- Cryptography - first thing that comes to their mind is exactly the number theory.
- practical private key cryptography is based on things like stream ciphers, block ciphers, and hash functions, that can be constructed analyzed, and reasoned about, without any mention of any number theory.

Contd…

- Public key world is different.
- Fast cryptography – efficient algorithms are required.
- Asymptotic complexity - the length of the input.

Contd…

- And in particular if we have some input integer A then the magnitude of A is itself. If A is equal to 1000 then the magnitude of A is 1000. But the length of that input, the length of A, is the length of the binary representation of A.
- Length of a is $||a|| = O(\log a)$
- Magnitude of a = $2^{||a||}$
- Algorithm is easy (P class) or hard(NP).

Contd…

- Add, sub, mul, div can be done efficiently
- modular addition, subtraction, multiplication, and reduction can be done efficiently.
- compute integer exponentiation is required.

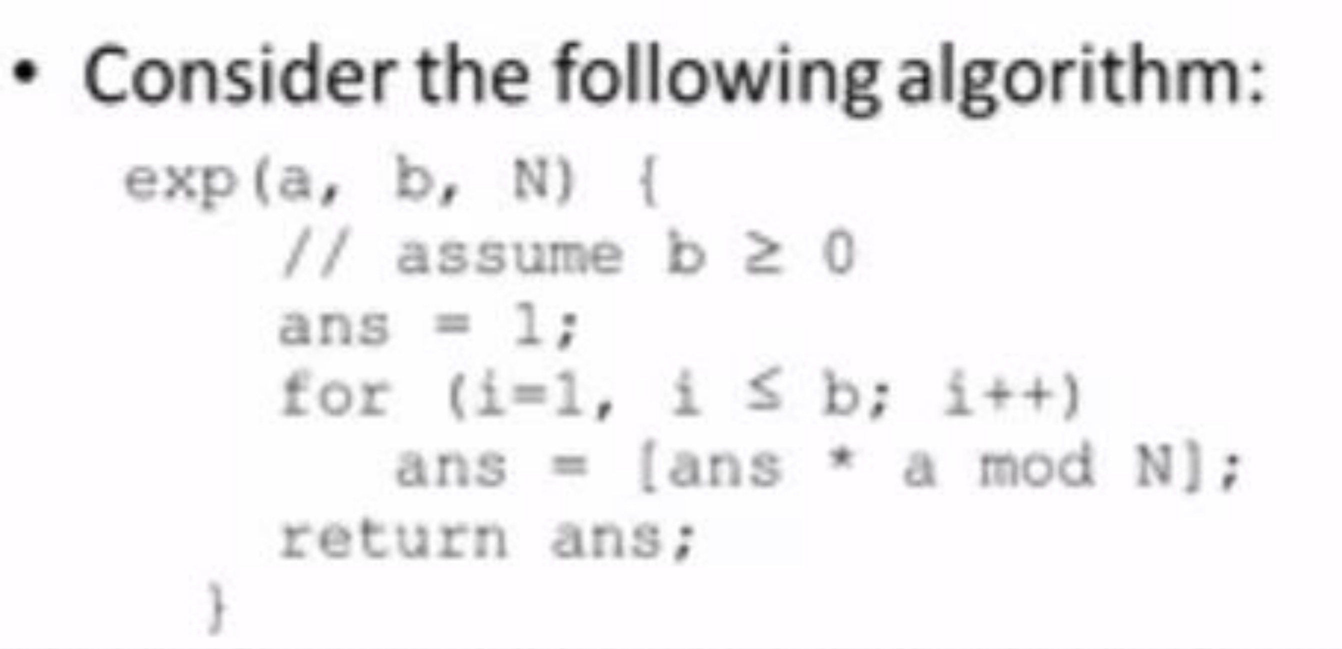
Contd…

- a^b, $||a^b|| = O(b.||a||)$
- naive algorithm - does not run in polynomial time,
- but with a little bit of cleverness you can come up with an algorithm that does run in polynomial time.

Contd…

- Compute a^{b} mod N.
- Computing a^b is not possible.

Contd…(B iterations)

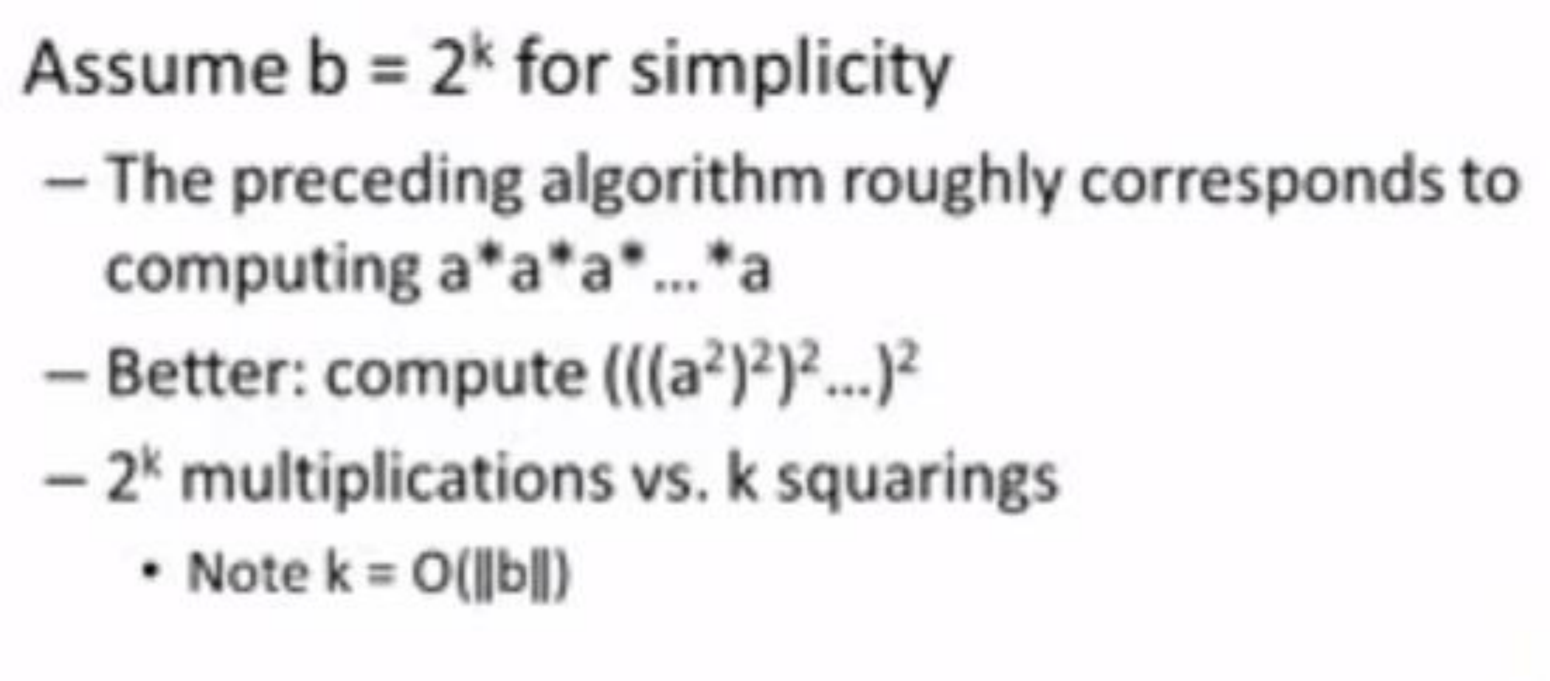


- Consider the following algorithm:

```
exp(a, b, N) {
    // assume b ≥ 0
    ans = 1;
    for (i=1, i ≤ b; i++)
        ans = [ans * a mod N];
    return ans;
  }
```

Efficient algorithm

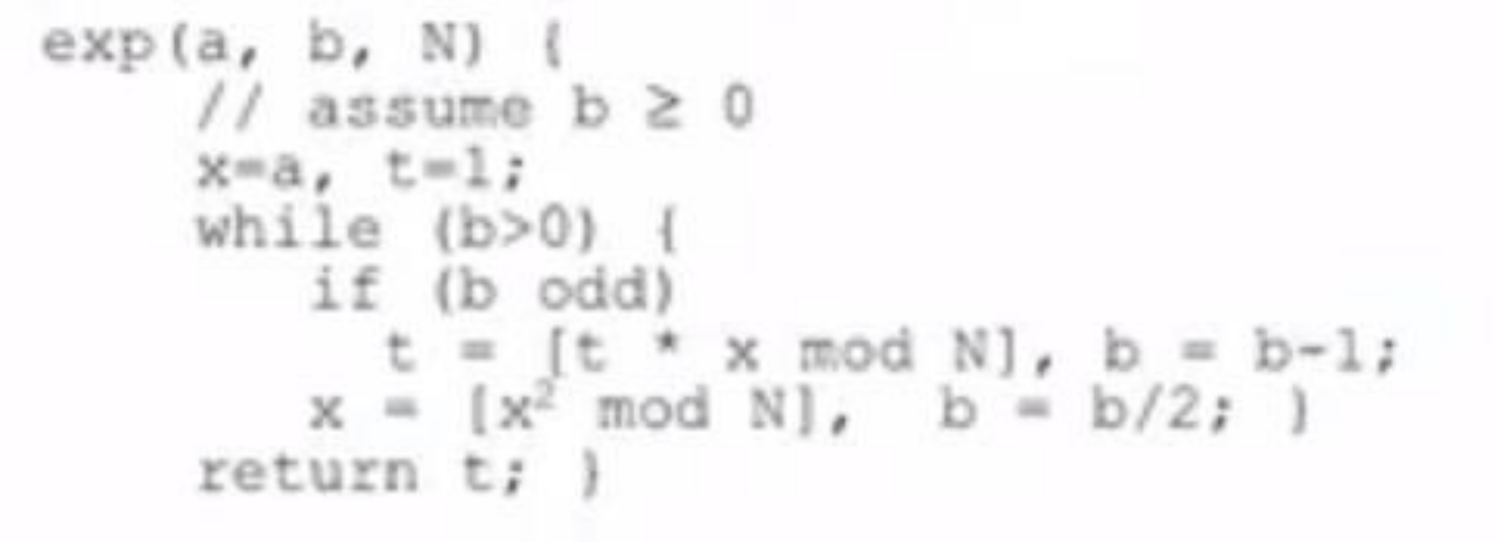
- $b = 2^k$



Assume $b = 2^k$ for simplicity

- The preceding algorithm roughly corresponds to computing a*a*a*…*a
- Better: compute $(((a^2)^2)^2\dots)^2$
- 2^k multiplications vs. k squarings
  - Note $k = O(\|b\|)$

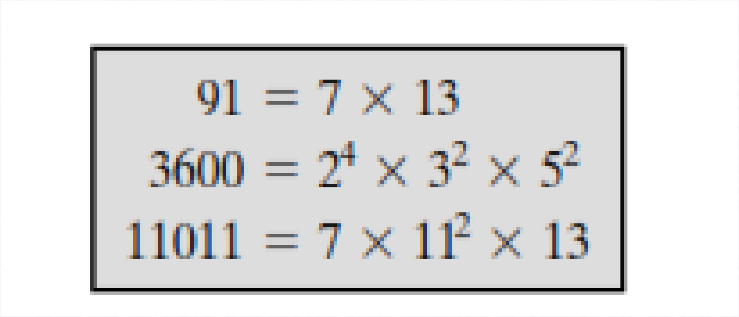
Contd...



```
exp(a, b, N) {
    // assume b ≥ 0
    x=a, t=1;
    while (b>0) {
        if (b odd)
            t = [t * x mod N], b = b-1;
        x = [$x^2$ mod N],  b = b/2; }
    return t; }
```

If b is odd, in first step subtract by 1, then it becomes even.

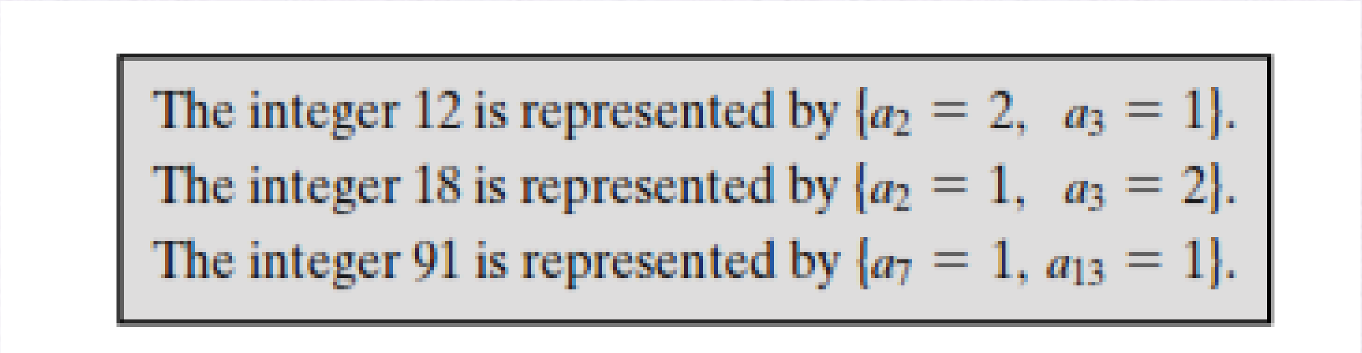
Contd…



$$91 = 7 \times 13$$

$$3600 = 2^4 \times 3^2 \times 5^2$$

$$11011 = 7 \times 11^2 \times 13$$



The integer 12 is represented by $\{a_2 = 2, \ a_3 = 1\}$.

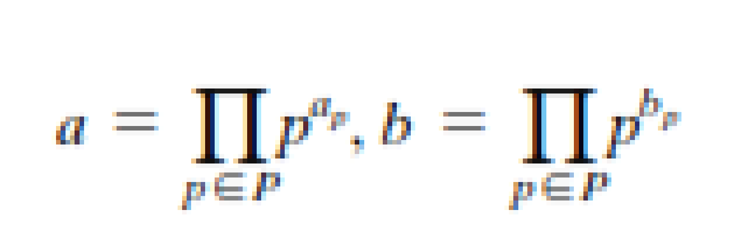
The integer 18 is represented by $\{a_2 = 1, \ a_3 = 2\}$.

The integer 91 is represented by $\{a_7 = 1, a_{13} = 1\}$.

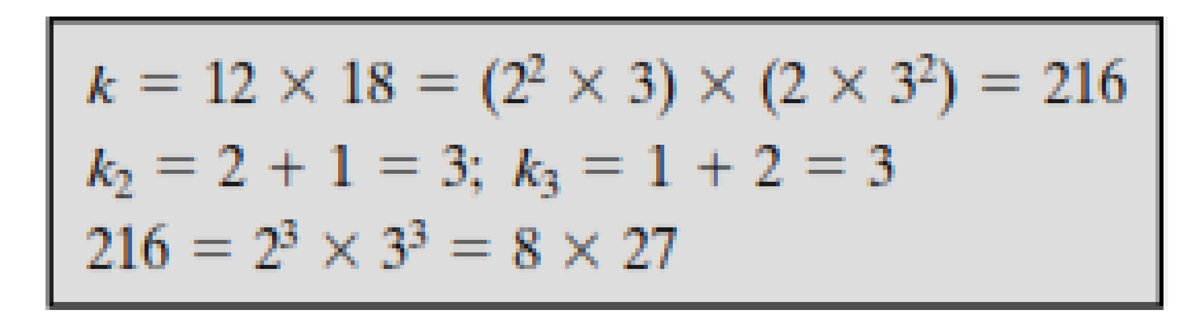
Table 8.1
Primes Under 2000

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Integer multiplication



$$a = \prod_{p \in P} p^{a_p}, b = \prod_{p \in P} p^{b_p}$$



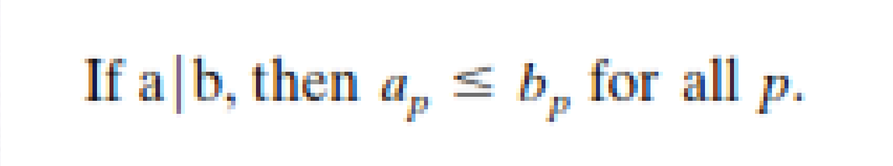
$k = 12 \times 18 = (2^2 \times 3) \times (2 \times 3^2) = 216$

$k_2 = 2 + 1 = 3;\ k_3 = 1 + 2 = 3$

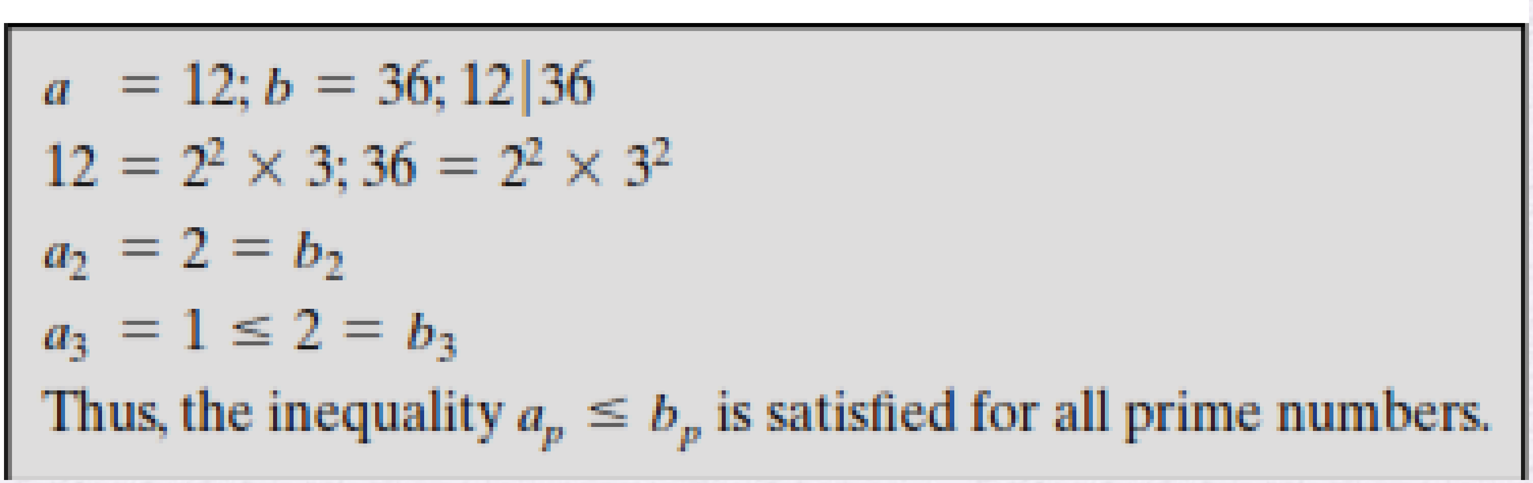
$216 = 2^3 \times 3^3 = 8 \times 27$

Contd…

- prime factors of *a and b, to say that a divides b?*



If a|b, then $a_p \leq b_p$ for all p.



$a = 12; b = 36; 12|36$

$12 = 2^2 \times 3; 36 = 2^2 \times 3^2$

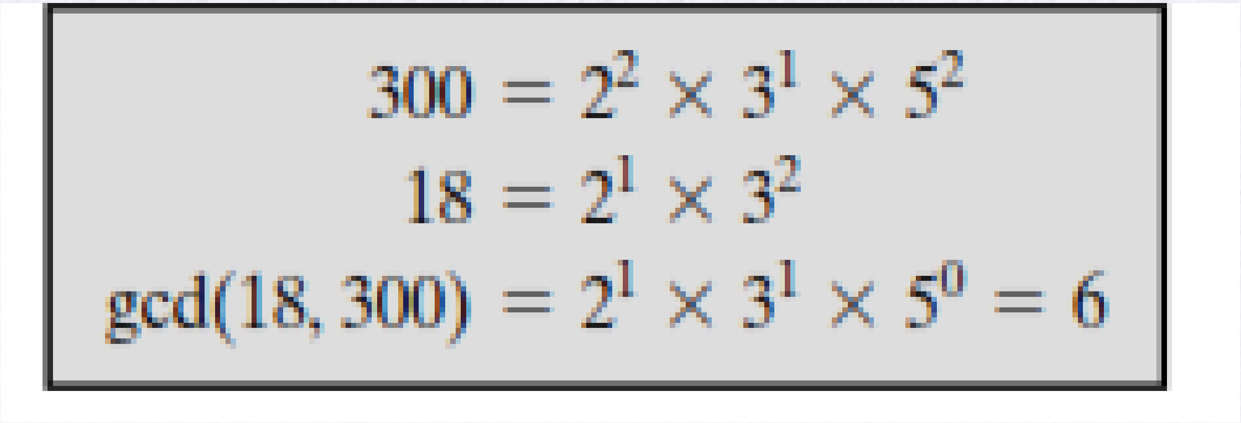
$a_2 = 2 = b_2$

$a_3 = 1 \leq 2 = b_3$

Thus, the inequality $a_p \leq b_p$ is satisfied for all prime numbers.

GCD

- greatest common divisor of two positive integers is the common product of primes, if we express each integer as the product of primes.



$$\begin{aligned} 300 &= 2^2 \times 3^1 \times 5^2 \\ 18 &= 2^1 \times 3^2 \\ \gcd(18, 300) &= 2^1 \times 3^1 \times 5^0 = 6 \end{aligned}$$

- Public-key cryptography uses Fermat’s theorem and Euler’s theorem.

Fermat's Theorem

- States the following:
  - If *p* is prime and *a* is a positive integer not divisible by *p* then

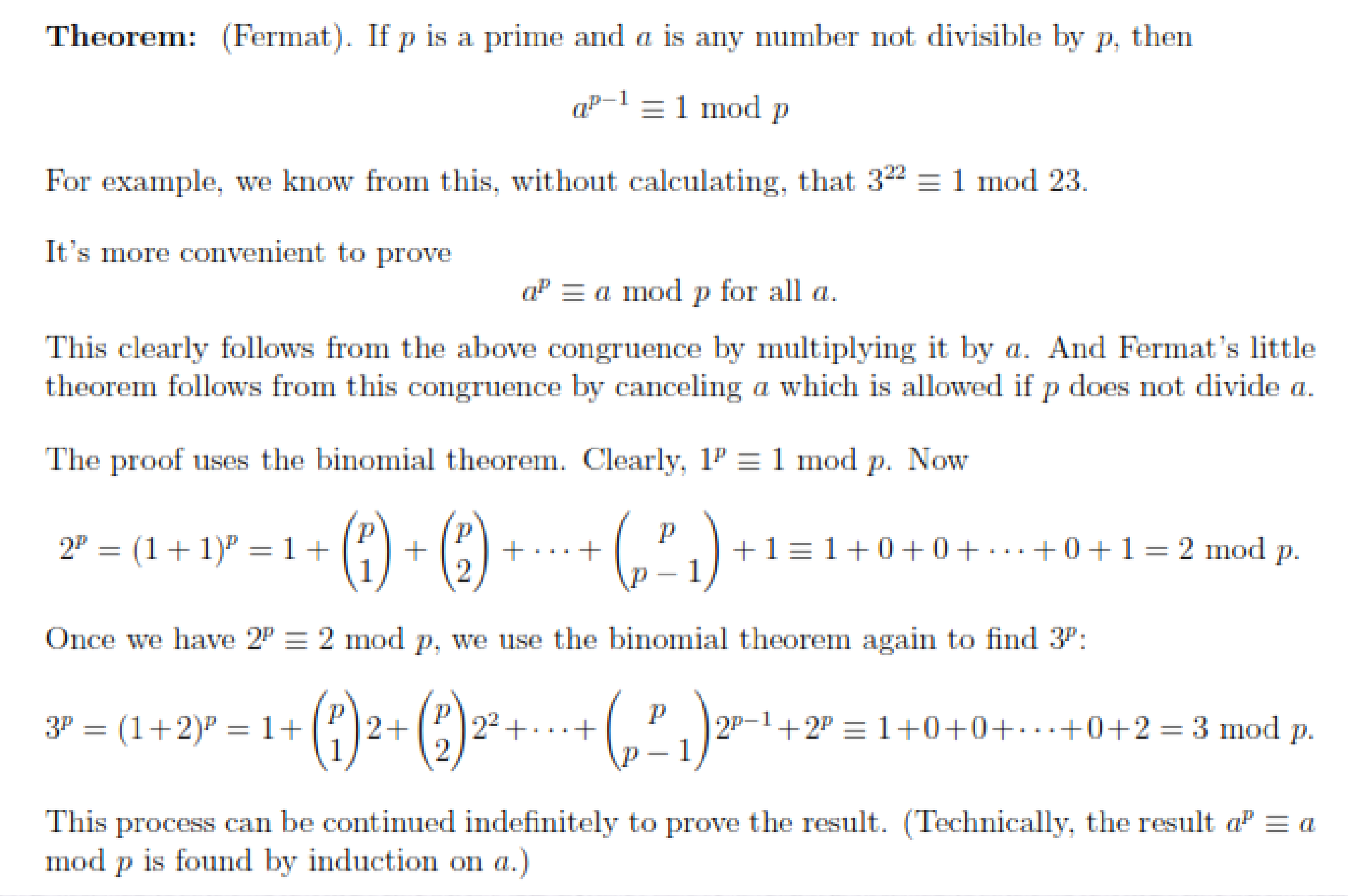
$$a^{p-1} = 1 \ (\text{mod } p)$$

- Sometimes referred to as Fermat’s Little Theorem
- An alternate form is:
  - If *p* is prime and *a* is a positive integer then

$$a^p = a \ (\text{mod } p)$$

- Plays an important role in public-key cryptography

Proof



Theorem: (Fermat). If p is a prime and a is any number not divisible by p, then

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

For example, we know from this, without calculating, that $3^{22} \equiv 1 \bmod 23$.

It's more convenient to prove

$$a^p \equiv a \bmod p \text{ for all } a.$$

This clearly follows from the above congruence by multiplying it by a. And Fermat's little theorem follows from this congruence by canceling a which is allowed if p does not divide a.

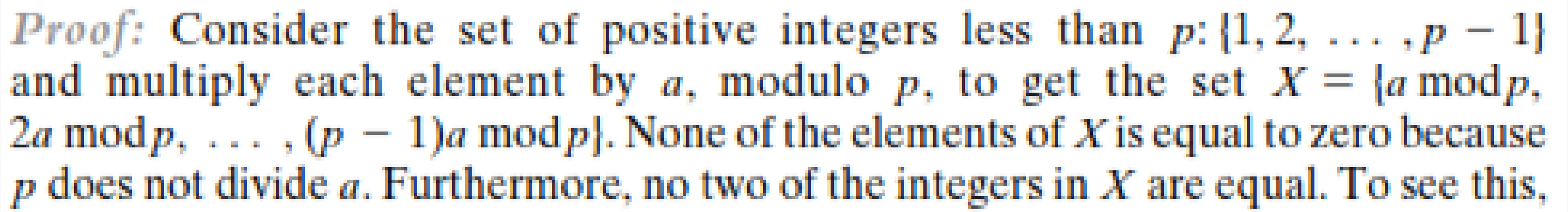
The proof uses the binomial theorem. Clearly, $1^p \equiv 1 \bmod p$. Now

$$2^p = (1+1)^p = 1 + \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1} + 1 \equiv 1 + 0 + 0 + \cdots + 0 + 1 = 2 \bmod p.$$

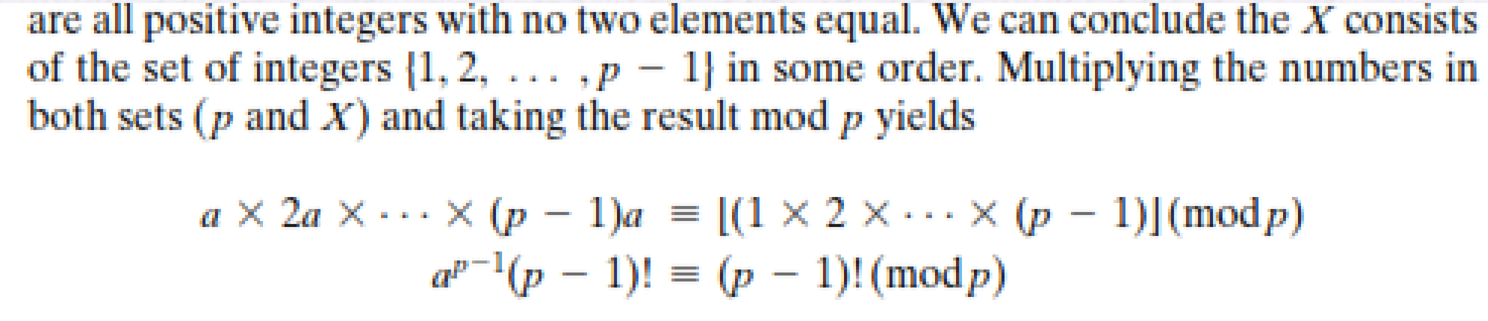
Once we have $2^p \equiv 2 \bmod p$, we use the binomial theorem again to find 3^p:

$$3^p = (1+2)^p = 1 + \binom{p}{1} 2 + \binom{p}{2} 2^2 + \cdots + \binom{p}{p-1} 2^{p-1} + 2^p \equiv 1 + 0 + 0 + \cdots + 0 + 2 = 3 \bmod p.$$

This process can be continued indefinitely to prove the result. (Technically, the result $a^p \equiv a \bmod p$ is found by induction on a.)

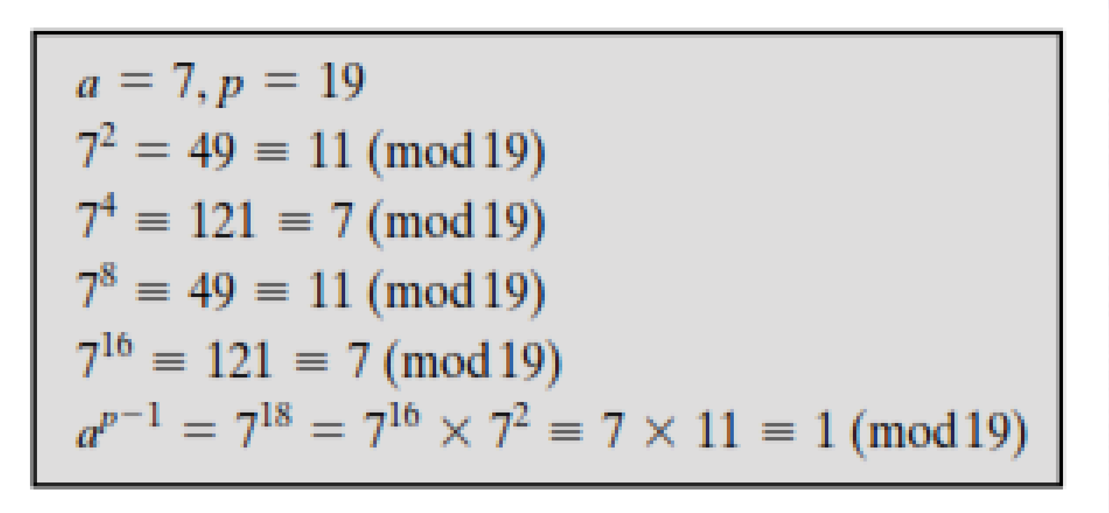


Proof: Consider the set of positive integers less than p: $\{1, 2, \ldots, p - 1\}$ and multiply each element by a, modulo p, to get the set $X = \{a \bmod p, 2a \bmod p, \ldots, (p - 1)a \bmod p\}$. None of the elements of X is equal to zero because p does not divide a. Furthermore, no two of the integers in X are equal. To see this,



are all positive integers with no two elements equal. We can conclude the X consists of the set of integers $\{1, 2, \ldots, p - 1\}$ in some order. Multiplying the numbers in both sets (p and X) and taking the result mod p yields

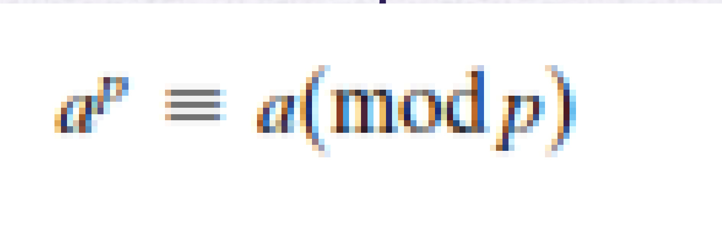
$$a \times 2a \times \cdots \times (p - 1)a \equiv [(1 \times 2 \times \cdots \times (p - 1)](\bmod p)$$
$$a^{p-1}(p - 1)! \equiv (p - 1)!(\bmod p)$$



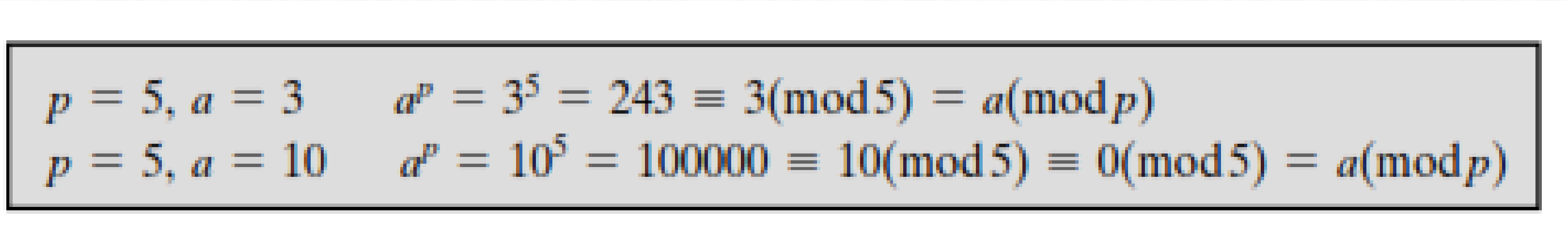
$$a = 7, p = 19$$
$$7^2 = 49 \equiv 11 \pmod{19}$$
$$7^4 \equiv 121 \equiv 7 \pmod{19}$$
$$7^8 \equiv 49 \equiv 11 \pmod{19}$$
$$7^{16} \equiv 121 \equiv 7 \pmod{19}$$
$$a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$$

2 power 16 mod 17

- If *p is prime and a is a* positive integer, then



$$a^p \equiv a(\bmod p)$$



$$p = 5, a = 3 \qquad a^p = 3^5 = 243 \equiv 3(\bmod 5) = a(\bmod p)$$

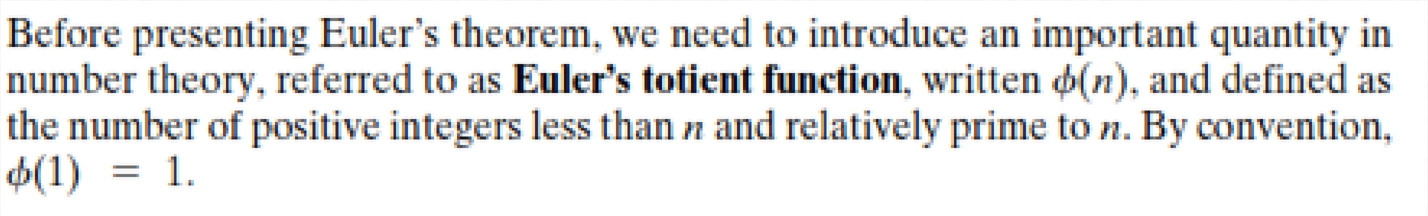
$$p = 5, a = 10 \qquad a^p = 10^5 = 100000 \equiv 10(\bmod 5) \equiv 0(\bmod 5) = a(\bmod p)$$

- **5555 to the power of 2222 + 2222 to the power of 5555 is divisible by 7?**

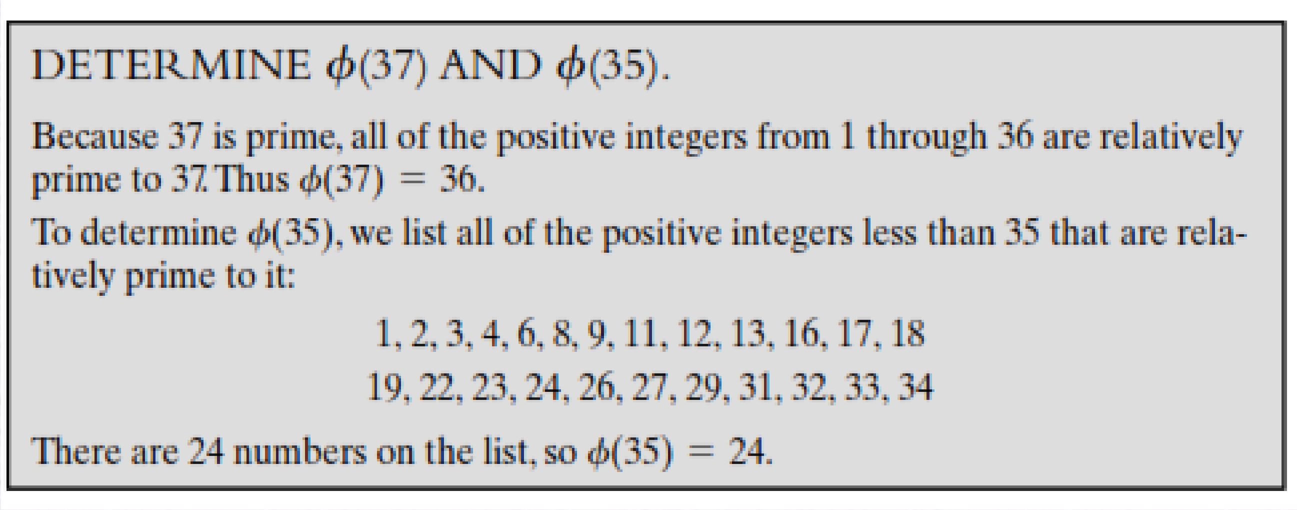
- 2222^1(mod 7) ≡ 3^1 ≡ 3
  2222^2(mod 7) ≡ 3^2 ≡ 2
  2222^3(mod 7) ≡ 3^3 ≡ 6
  2222^4(mod 7) ≡ 3^4 ≡ 4
  2222^5(mod 7) ≡ 3^5 ≡ 5
  2222^6(mod 7) ≡ 3^6 ≡ 1
  2222^7(mod 7) ≡ 3^7 ≡ 3

- 5555^1(mod 7) ≡ 4^1 ≡ 4
  5555^2(mod 7) ≡ 4^2 ≡ 2
  5555^3(mod 7) ≡ 4^3 ≡ 1
  5555^4(mod 7) ≡ 4^4 ≡ 4

Euler Totient Function



Before presenting Euler's theorem, we need to introduce an important quantity in number theory, referred to as **Euler's totient function**, written $\phi(n)$, and defined as the number of positive integers less than n and relatively prime to n. By convention, $\phi(1) = 1$.



DETERMINE $\phi(37)$ AND $\phi(35)$.

Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37.Thus $\phi(37) = 36$.

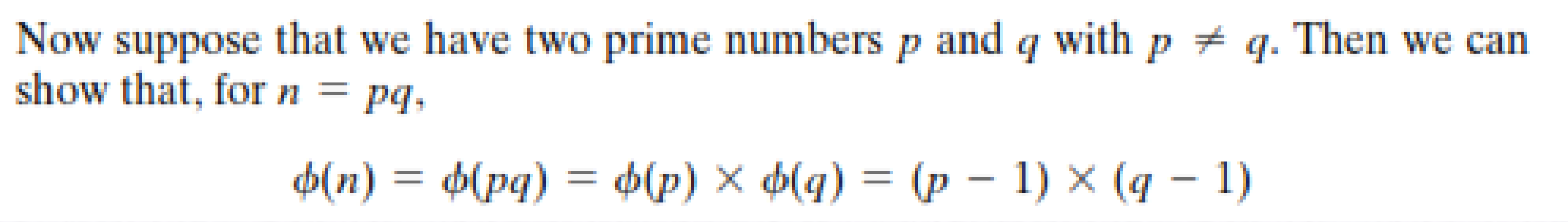
To determine $\phi(35)$, we list all of the positive integers less than 35 that are relatively prime to it:

$$1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18$$
$$19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34$$

There are 24 numbers on the list, so $\phi(35) = 24$.

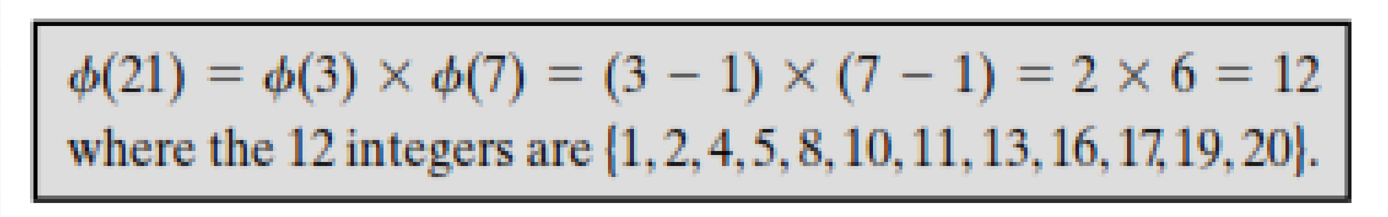
$$\phi(p) = p - 1$$

Contd…



Now suppose that we have two prime numbers p and q with $p \neq q$. Then we can show that, for $n = pq$,

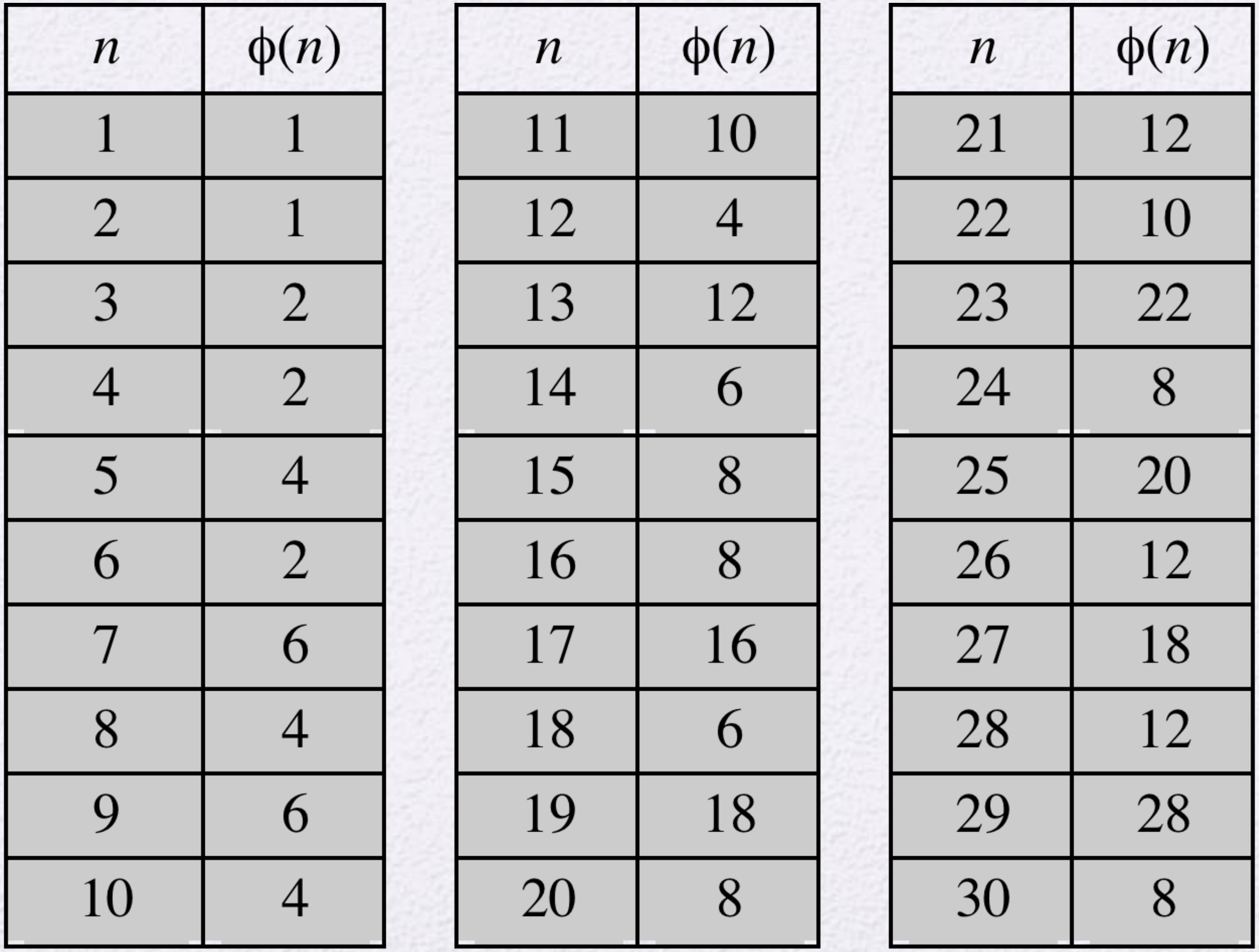
$$\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p - 1) \times (q - 1)$$



$\phi(21) = \phi(3) \times \phi(7) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$
where the 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

Table 8.2

Some Values of Euler's Totient Function ø(*n*)



n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

Euler's Theorem

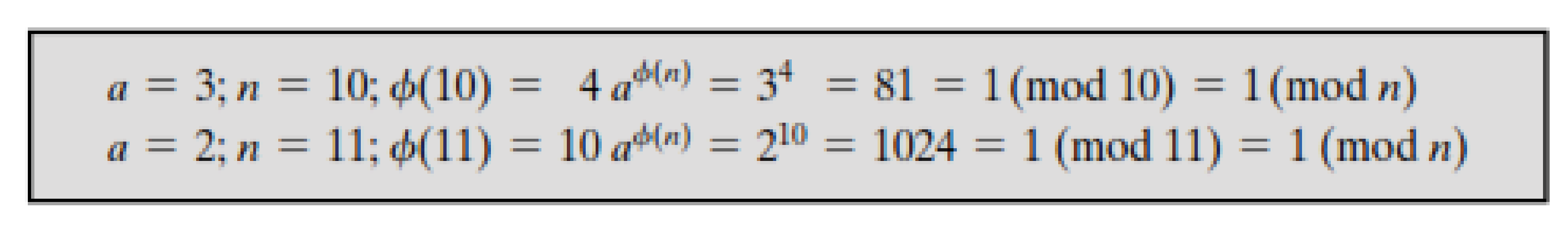
- States that for every *a* and *n* that are relatively prime:

$$a^{\varnothing(n)} = 1(\mathrm{mod}\ n)$$

- An alternative form is:

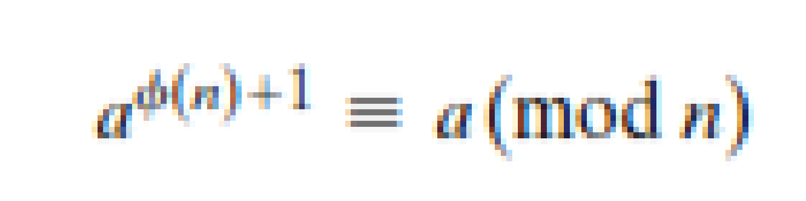
$$a^{\varnothing(n)+1} = a(\mathrm{mod}\ n)$$

- Plays an important role in public-key cryptography



$$a = 3;\ n = 10;\ \phi(10) = 4\ a^{\phi(n)} = 3^4 = 81 = 1\,(\mathrm{mod}\ 10) = 1\,(\mathrm{mod}\ n)$$

$$a = 2;\ n = 11;\ \phi(11) = 10\ a^{\phi(n)} = 2^{10} = 1024 = 1\ (\mathrm{mod}\ 11) = 1\ (\mathrm{mod}\ n)$$



$$a^{\phi(n)+1} \equiv a\,(\mathrm{mod}\ n)$$

Miller-Rabin Algorithm

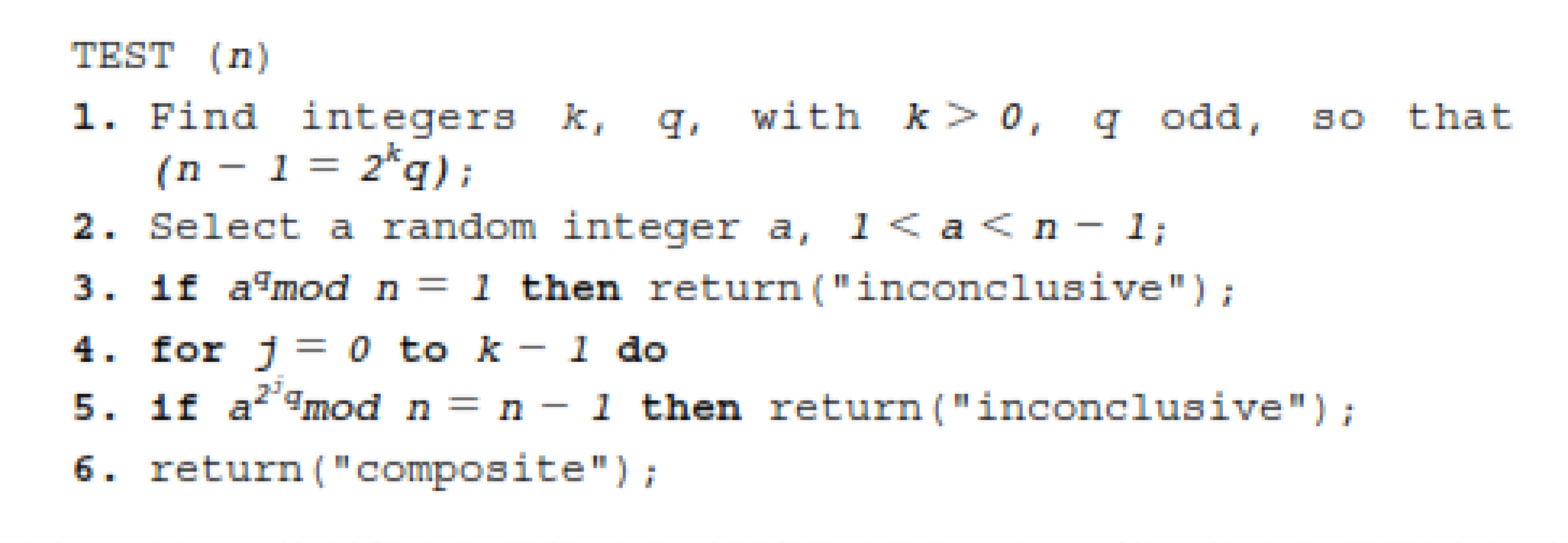
- Typically used to test a large number for primality

- Algorithm is:

TEST (n)

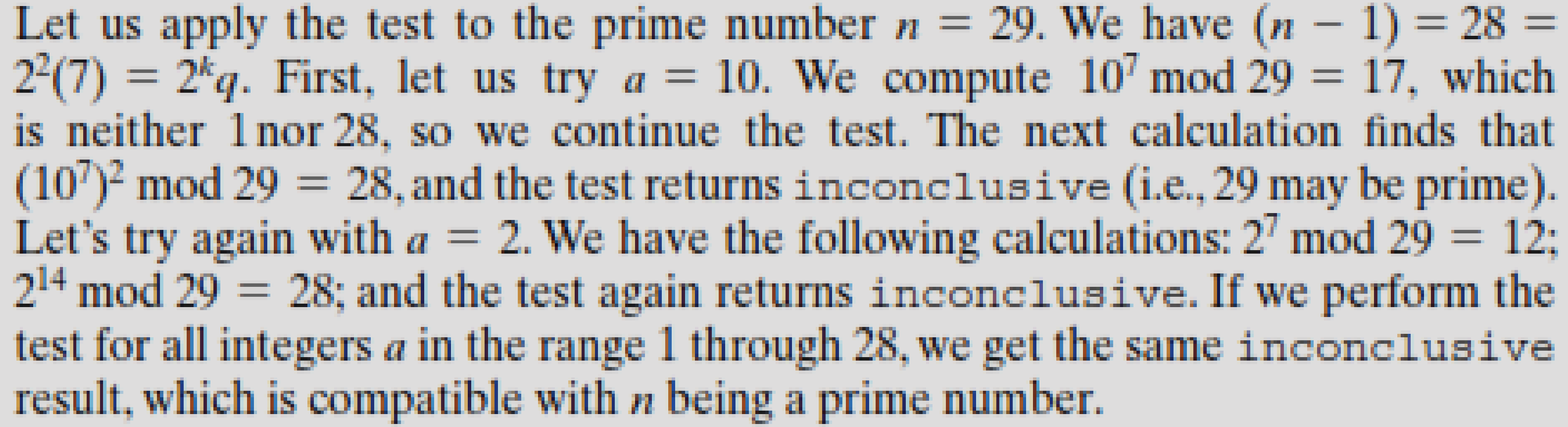
```
1. • Find integers $k$, $q$, with $k > 0$, $q$ odd, so that $(n - 1)=2^kq$ ;
2. • Select a random integer $a$, $1 < a < n - 1$ ;
3. • **if** $a^q \bmod n = 1$ **then** return ("inconclusive") ;
4. • **for** $j = 0$ **to** $k - 1$ **do**
5.     • **if** $(a^{2^jq} \bmod n = n - 1)$ **then** return ("inconclusive") ;
6. • return ("composite") ;
```

Contd…

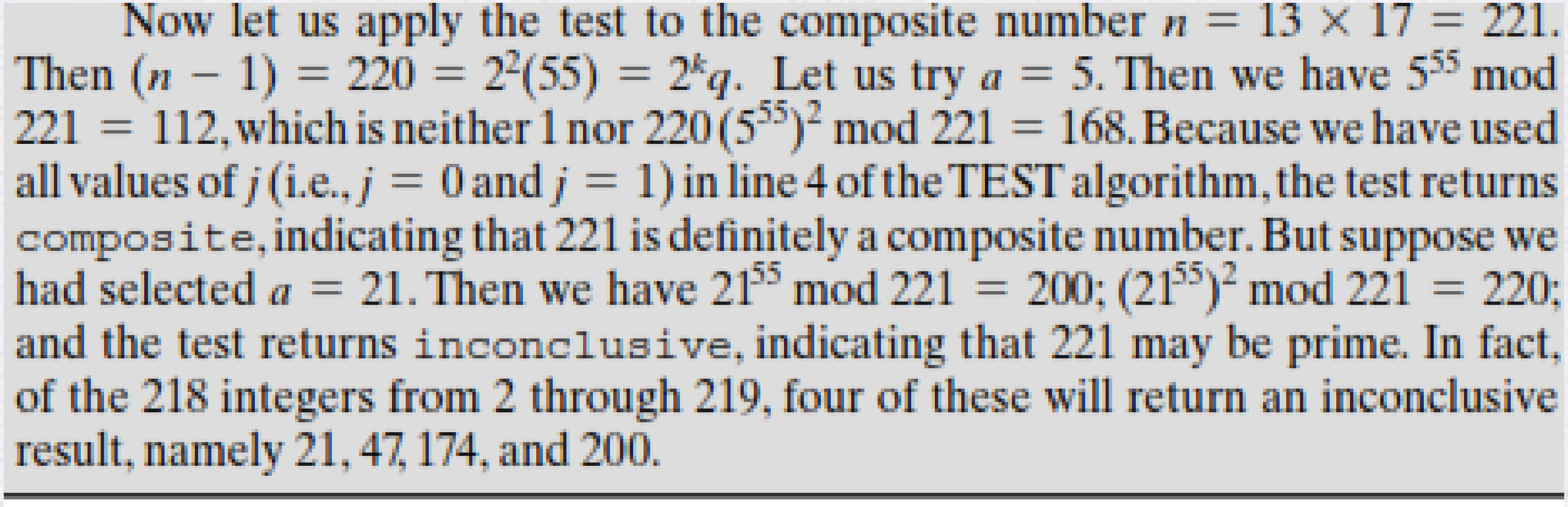


```
TEST ($n$)
1. Find integers $k$, $q$, with $k > 0$, $q$ odd, so that
   ($n - 1 = 2^k q$);
2. Select a random integer $a$, $1 < a < n - 1$;
3. if $a^q mod\ n = 1$ then return("inconclusive");
4. for $j = 0$ to $k - 1$ do
5. if $a^{2^j q} mod\ n = n - 1$ then return("inconclusive");
6. return("composite");
```

Contd...



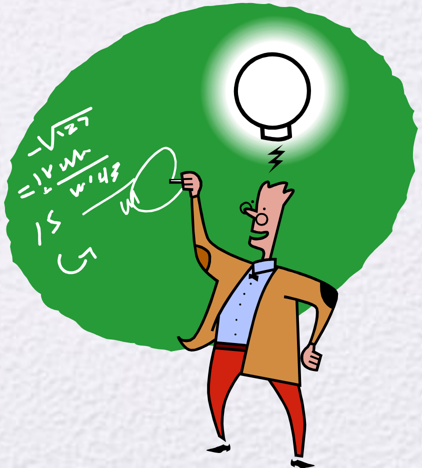
Let us apply the test to the prime number $n = 29$. We have $(n - 1) = 28 = 2^2(7) = 2^k q$. First, let us try $a = 10$. We compute $10^7 \bmod 29 = 17$, which is neither 1 nor 28, so we continue the test. The next calculation finds that $(10^7)^2 \bmod 29 = 28$, and the test returns `inconclusive` (i.e., 29 may be prime). Let's try again with $a = 2$. We have the following calculations: $2^7 \bmod 29 = 12$; $2^{14} \bmod 29 = 28$; and the test again returns `inconclusive`. If we perform the test for all integers a in the range 1 through 28, we get the same `inconclusive` result, which is compatible with n being a prime number.



Now let us apply the test to the composite number $n = 13 \times 17 = 221$. Then $(n - 1) = 220 = 2^2(55) = 2^kq$. Let us try $a = 5$. Then we have 5^{55} mod $221 = 112$, which is neither 1 nor 220 $(5^{55})^2$ mod $221 = 168$. Because we have used all values of j (i.e., $j = 0$ and $j = 1$) in line 4 of the TEST algorithm, the test returns `composite`, indicating that 221 is definitely a composite number. But suppose we had selected $a = 21$. Then we have 21^{55} mod $221 = 200$; $(21^{55})^2$ mod $221 = 220$; and the test returns `inconclusive`, indicating that 221 may be prime. In fact, of the 218 integers from 2 through 219, four of these will return an inconclusive result, namely 21, 47, 174, and 200.

Deterministic Primality Algorithm

- Prior to 2002 there was no known method of efficiently proving the primality of very large numbers
- All of the algorithms in use produced a probabilistic result
- In 2002 Agrawal, Kayal, and Saxena developed an algorithm that efficiently determines whether a given large number is prime
  - Known as the AKS algorithm
  - Does not appear to be as efficient as the Miller-Rabin algorithm



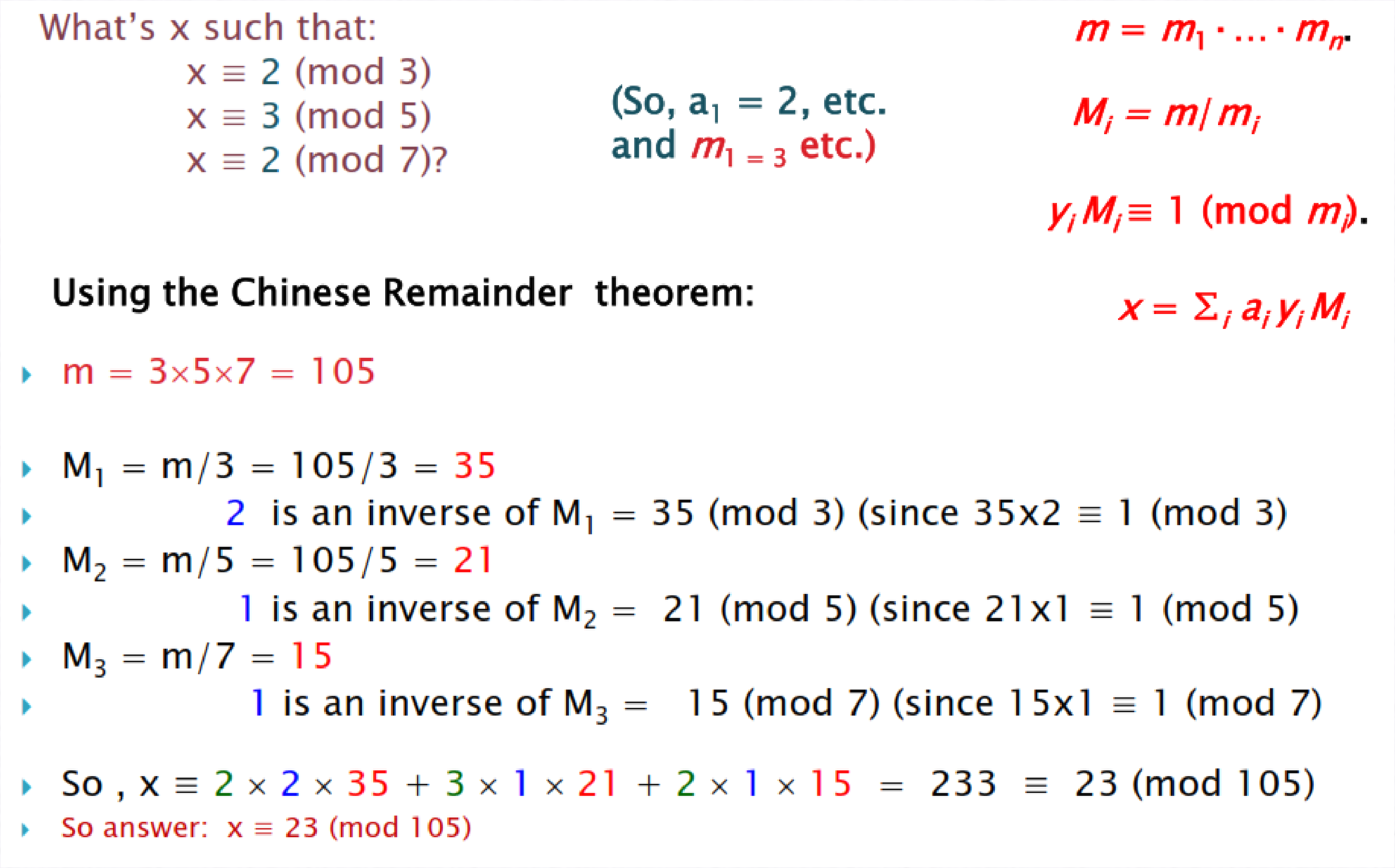
Chinese Remainder Theorem (CRT)

- Believed to have been discovered by the Chinese mathematician Sun-Tsu in around 100 A.D.
- One of the most useful results of number theory
- Says it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli
- Can be stated in several ways

Provides a way to manipulate (potentially very large) numbers mod *M* in terms of tuples of smaller numbers

- This can be useful when *M* is 150 digits or more
- However, it is necessary to know beforehand the factorization of *M*

Example



What's x such that:

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$?

(So, $a_1 = 2$, etc.
and $m_1 = 3$ etc.)

$m = m_1 \cdot \ldots \cdot m_n$.

$M_i = m / m_i$

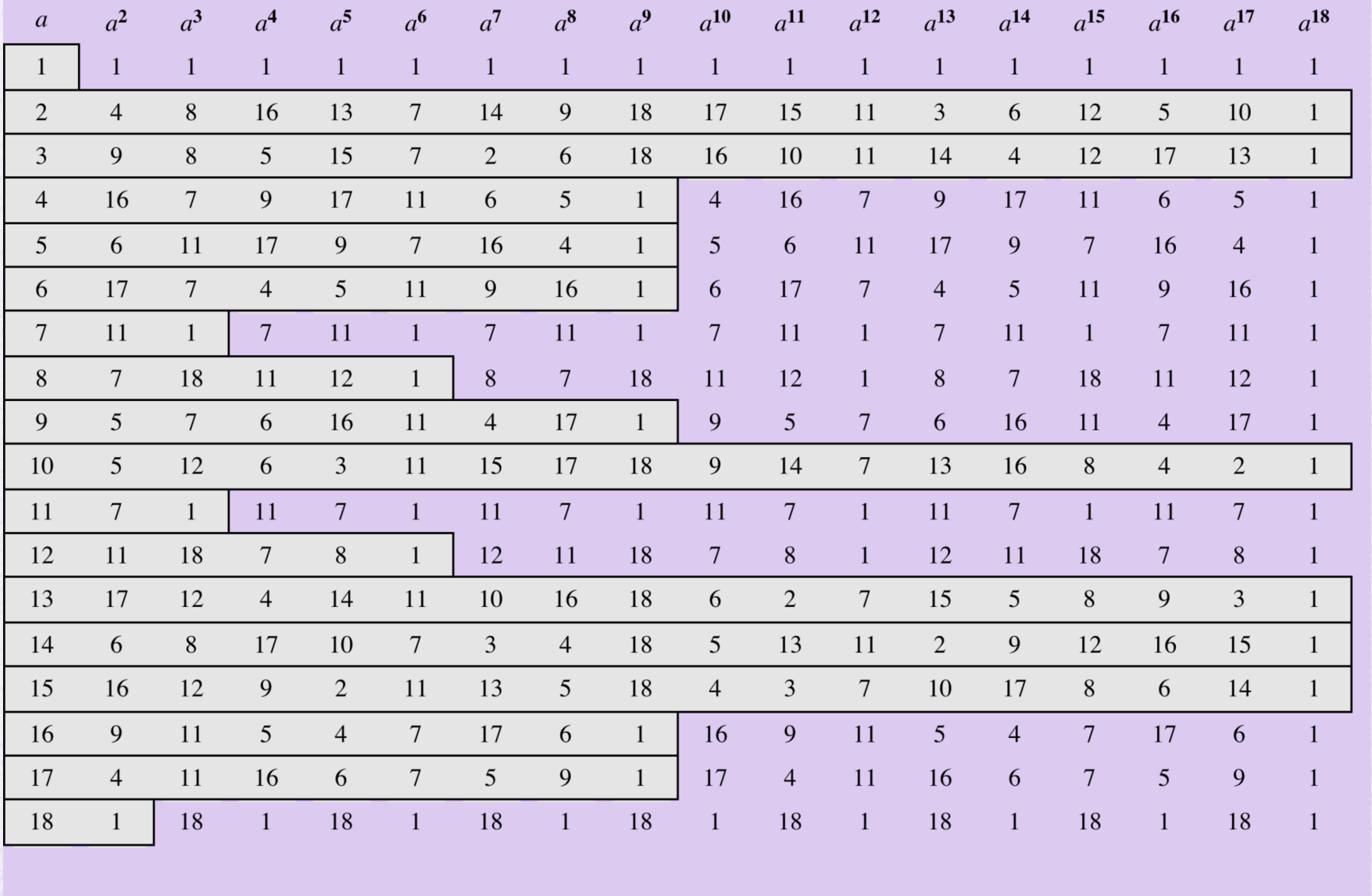
$y_i M_i \equiv 1 \pmod{m_i}$.

Using the Chinese Remainder theorem:

$x = \Sigma_i a_i y_i M_i$

- $m = 3 \times 5 \times 7 = 105$
- $M_1 = m/3 = 105/3 = 35$
- 2 is an inverse of $M_1 = 35 \pmod 3$ (since $35x2 \equiv 1 \pmod 3$
- $M_2 = m/5 = 105/5 = 21$
- 1 is an inverse of $M_2 = 21 \pmod 5$ (since $21x1 \equiv 1 \pmod 5$
- $M_3 = m/7 = 15$
- 1 is an inverse of $M_3 = 15 \pmod 7$ (since $15x1 \equiv 1 \pmod 7$
- So , $x \equiv 2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15 = 233 \equiv 23 \pmod{105}$
- So answer: $x \equiv 23 \pmod{105}$

Table 8.3
Powers of Integers, Modulo 19



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}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Table 8.4 Tables of Discrete Logarithms, Modulo 19

(a) Discrete logarithms to the base 2, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(b) Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(c) Discrete logarithms to the base 10, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

(d) Discrete logarithms to the base 13, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(e) Discrete logarithms to the base 14, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9

(f) Discrete logarithms to the base 15, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

Summary

- Prime numbers
- Fermat’s Theorem
- Euler’s totient function
- Euler’s Theorem
- Testing for primality
  - Miller-Rabin algorithm
  - A deterministic primality algorithm
  - Distribution of primes

- The Chinese Remainder Theorem
- Discrete logarithms
  - Powers of an integer, modulo *n*
  - Logarithms for modular arithmetic
  - Calculation of discrete logarithms