1. Modular arithmetic

1.1. **Divisibility.** Given positive numbers a, b, if $a \neq 0$ we can write

$$b = aq + r$$

for appropriate integers q, r such that $0 \leq r \leq a$. [1] The number r is the **remainder**. We say that a **divides** b (or $a|b$) if $r = 0$ and so $b = aq$ i.e. b factors as a times q.

1.2. **Primes.** A number is **prime** if it can't be factored (as a product of two numbers greater or equal to 2). If a number factors (i.e. it is not prime), then we say that it is **composite**.

Exercise 1.1. Find all prime numbers smaller than 100.

Here are several important questions:

(1) How do we determine whether a number is prime?
(2) How do we factor a number into primes?
(3) How can we find big prime numbers?
(4) How many prime numbers are there?

Exercise 1.2. Factor 12, 123, 1234, 1235, 1236, 128417.

Exercise 1.3. Show that every number is either prime or divisible by a prime number.

Theorem 1.4. *There are infinitely many prime numbers.*

Proof. Suppose that there are only finitely many prime numbers $P_1, \cdots, P_n$, then $N = P_1 \cdot P_2 \cdots P_n + 1$ is not divisible by any prime, hence it does not factor and hence it is a new prime! □

1.3. **Divisibility tricks.** Recall that a number is even if its last digit is divisible by 2, it is divisible by 3 if the sum of its digits is divisible by 3, it is divisible by 5 if its last digit is divisible by 5 etc.

Why is this? Can we find other divisibility tricks (eg. for 7)?

One possible explanation. Let abc be a 3 digit number so that $abc = a \cdot 100 + b \cdot 10 + c \cdot 1$. Then

$abc/2 = a \cdot 50 + b \cdot 5 + c/2$ and this is an integer only if $c/2$ is an integer.

$abc/5 = a \cdot 20 + b \cdot 2 + c/5$ and this is an integer only if $c/5$ is an integer.

$abc/3 = a \cdot 33 + b \cdot 3 + (a + b + c)/3$ and this is an integer only if $(a + b + c)/3$ is an integer.

A better explanation is given by congruences.

[1] In Python notation $r = b\%a$ and $q = b//a$.

1.4. **Congruences.** We say that a is congruent to b modulo N i.e. $a \equiv b \ mod \ N$ iff N divides $a-b$ or equivalently iff $a\%N = b\%N$. So a is congruent modulo N to any number in the arithmetic progression

$$\{\cdots a-2N, a-N, a, a+N, a+2N\cdots\}.$$

Here are some examples

1. $273 \equiv 593 \ mod \ 10$
2. $273 \not\equiv 593 \ mod \ 100$
3. $359 \equiv 2 \ mod \ 17$
4. $216 \equiv 12 \ mod \ 17$

Exercise 1.5. Is 71651 divisible by 3? How about 771651 ?

Exercise 1.6. (1) What is the last digit of 273^{100}?

(2) Of 273^{111}?

(3) What are the last two digits of the numbers above?

Solution: Every integer modulo 10 is congruent to one of:

$$\{0, 1, 2, \cdots, 9\}.$$

we call this a system of residues modulo 10. We now compute the residue of 273^{100}. We have:

$$273 \equiv 3, \qquad 273^2 \equiv 9, \qquad 273^3 \equiv 27 \equiv 7, \qquad 273^4 \equiv 1.$$

Then

$$273^{100} = (273^4)^{25} = 1^{25} = 1.$$

1.5. **Arithmetic of residues (modular arithmetic).** Residues modulo 5: $\{0, 1, 2, 3, 4\} = \mathbb{Z}/5$.

Exercise 1.7. Write down the addition and multiplication tables.

We can compute $3 * 4 = 2$, $3 + 3 = 1$ etc. We have

$$0 = -0, \ 4 = -1, \ 3 = -2, \ 2 = -3, \ 1 = -4.$$

Check $0+0 = 0$, $1+4 = 0$, $2+3 = 0$. Now a/b makes little sense (eg. what does $3/4$ mean?). We should write $a * b^{-1}$, eg. $3 * 4^{-1}$. From the multiplication table, we see that $4 * 4 = 1$ so that $4^{-1} = 4$ and then

$$3 * 4^{-1} = 3 * 4 = 2.$$

Exercise 1.8. (1) Write down the addition and multiplication tables for $\mathbb{Z}/7$, $\mathbb{Z}/8$.

(2) Find the additive and multiplicative inverses of 5 mod 11, 7 mod 23, 7 mod 101 and 4 mod 8.

(3) Find the order of 359 mod 17.

(4) Find the orders of $2, 3, \cdots, 9$ mod 11. Do you see a pattern?

(5) Can you solve $x^2 = 5$ mod 11? and $x^2 = 6$ mod 11?

(6) Show that if $a \equiv b$, $c \equiv d$ then $a + b \equiv b + d$ and $ac \equiv bd$.

2. The Euclidean Algorithm

2.1. **The greatest common divisor.** By definition the greatest common divisor of two numbers a, b is the largest number that divides both a and b. We denote it by $GCD(a, b)$ or just by (a, b). Eg $(7, 11) = 1$, $(10, 15) = 5$, $(5555, 7931) = 11$. To see the last one, write $5555 = 5*11*101$ and $7931 = 7*11*103$ so that the sets of divisors are $\{1, 5, 11, 55, 101, 505, 1111, 5555\}$ and $\{1, 7, 11, 77, 103, 721, 1133, 7931\}$.

We can compute the GCD in the following ways:

(1) By brute force: Find all the divisors and compare.
(2) Find all divisors of a and throw out the ones that do not divide b.
(3) Compare prime factors and multiply the highest powers that divide both numbers.
(4) The Euclidean algorithm.

The Euclidean algorithm is by far the fastest method (for big numbers).

2.2. **The Euclidean algorithm.** Start with $a = 2310$, $b = 1547$ and let $r = a\%b$ be the remainder. Replace a by b and b by r and repeat. The last nonzero remainder is the GCD.

a	b	r	q
2310	1547	763	1
763	21	7	36
21	7	0	3

The GCD is 7.

Exercise 2.1. Find the GCD of 12345, 54321 and of 45201647, 18296431.

Exercise 2.2. Factor the above numbers.

2.3. **Python Code.**

```
def gcd(a,b):
  r=a%b
  print a,b,r
  while r>0:
    a,b,r = b,r,b%r
    print a,b,r
  return b
```

It works as follows:

```
>>> gcd(2310,1547)
2310 1547 763
1547 763 21
763 21 7
21 7 0
7
```

2.4. **Well ordering principle.** *Each nonempty set of positive integers has a least element.*

Note that this is not true for the rationals. Eg. $\mathbb{Q}_{>0}$ has no smallest number.

Proposition 2.3. *Given positive integers a, b, let $S = \{ax + by > 0\}$ where x, y are any integers. Let g be the least element in S, then $g = GCD(a, b)$.*

Proof. It is enough to show that g divides $GCD(a, b)$ and that $GCD(a, b)$ divides g.

Clearly $GCD(a, b)$ divides a and b so it divides any element in S and so it divides g.

To see that g divides $GCD(a, b)$ it is enough to show that g divides a (and that g divides b). Consider $a = gq + r$, then $r = a - gq = a - (ax + by)q = (1 - q)ax - (bq)y$. Now $0 \leq r < g$ and so $r = 0$ (else $r \in S$ contradicting the fact that g is the smallest element of S). Therefore g divides a (and by the same argument it divides b) and so it divides $GCD(a, b)$. □

So we can always write

$$GCD(a, b) = ax + by.$$

This allows us to find the inverse of any number $1 \leq a \leq p - 1$ modulo p when p is prime. In fact $GCD(a, p) = 1$ so we have $1 = ax + py$ so modulo p we have $1 \equiv ax$ i.e. $x = a^{-1}$ modulo p.

2.5. **Finding x and y.** Use back substitution! Eg. for $a = 2310$, $b = 1547$ then $GCD(a, b) = 7$. Recall that

a	b	r	q
2310	1547	763	1
1547	763	21	2
763	21	7	36
21	7	0	3

So $763 = 2310 - 1547$, $21 = 1547 - 2 * 763$ and $7 = 763 - 36 * 21$. Then

$$7 = 763 - 36 * 21 = 763 - 36 * (1547 - 2 * 763) = 73 * 763 - 36 * 1547 =$$

$$73 * (2310 - 1547) - 36 * 1547 = 73 * 2310 - 109 * 1547.$$

Exercise 2.4. Solve

(1) $54321x + 12345y = 3$
(2) $54321x + 12346y = 1$.

Exercise 2.5. Find the multiplicative inverse of

(1) 44 mod 123
(2) 444 mod 1234567.

2.6. **Python code for the Extended Euclidean Algorithm.** .

```
def egcd(a,b):
  q,r = divmod(a,b)
  x,y,u,v=1,-q,0,1
  while r>0:
    qq,rr = divmod(b,r)
    xx,yy=u-qq*x,v-qq*y
    a,b,r,q,x,y,u,v=b,r,rr,qq,xx,yy,x,y
    print a,b,r,q,x,y,u,v
  return u,v,b
```

Exercise 2.6. What are the last 4 digits of the multiplicative inverse of 17 mod 10^{100}?

Exercise 2.7. I have encoded my SSN using the algorithm $f(x) = 103x \bmod 10^{10}$. The result is 3536767732. What is my SSN? (You will need a calculator that can compute with 20 digit numbers, eg, python.)

3. Modular Powers

We begin by writing a table for the powers modulo 3, 5, 7.

Modulo 3

a	a^2	a^3	a^4	a^5	a^6	a^7
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	1	2	1	2	1	2

Note that after we get a column with all 1's (and a 0 at the top), the pattern must repeat. Therefore, as soon as (and if) this happens, the table just keeps repeating itself (and so we do not bother to keep writing the repeated entries).

Modulo 5

a	a^2	a^3	a^4	a^5	a^6	a^7
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	4	3	1	2	4	3
3	4	2	1	3	4	2
4	1	4	1	4	1	4

Here, the 4th column has all 1's (and a 0 at the top).

Modulo 7

a	a^2	a^3	a^4	a^5	a^6	a^7
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	4	1	2	4	1	2
3	2	6	4	5	1	3
4	2	1	4	2	1	4
5	4	6	2	3	1	5
6	1	6	1	6	1	6

Do you notice a pattern? The first pattern, seems to be that for all $a \neq 0$ we have $a^2 \equiv 1 \bmod 3$; $a^4 \equiv 1 \bmod 5$; $a^6 \equiv 1 \bmod 7$. It is easy to guess what the general pattern might be:

Theorem 3.1 (Fermat's Little Theorem). *Let p be any prime and $0 < a < p$. Then*

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

Eg. $6^{22} \equiv 1 \bmod 23$. (Check: $6^{22} = 23 \cdot 572268277 + 1$.) Similarly $84^{100} \equiv 1 \bmod 101$. (Note that 84^{100} has more than 100 digits, so checking explicitly might not be so easy!)

Proof. We claim that the set $\{a, 2a, \cdots, (p-1)a\}$ is the same as the set $\{1, 2, \cdots, p-1\}$ (the elements are not in the same order!). Granting the claim, then we have

$$1 \cdot 2 \cdots (p-1) = a \cdot 2a \cdots (p-1)a = 1 \cdot 2 \cdots (p-1) \cdot a^{p-1}.$$

Since p does not divide $1 \cdot 2 \cdots (p-1)$, it follows that $GCD(p, 1 \cdot 2 \cdots (p-1)) = 1$, so there is a number $1 \leq x \leq p-1$ such that $x \cdot 1 \cdot 2 \cdots (p-1) \equiv 1 \bmod p$. But then

$$1 \equiv x \cdot 1 \cdot 2 \cdots (p-1) \equiv x \cdot 1 \cdot 2 \cdots (p-1) \cdot a^{p-1} \equiv a^{p-1}$$

as required.

To see the claim, we must check that
1) The map $x \to ax \bmod p$ induces a map

$$\{1, 2, \cdots, p-1\} \to \{a, 2a, \cdots, (p-1)a\}.$$

I.e. that for all $1 \leq x \leq p-1$, we have that p does not divide ax. This is clear as p is a prime number that does not divide either of a and x.
2) If $1 \leq x \neq y \leq p-1$ then $ax \neq ay \bmod p$ (i.e. this function is 1 to 1). Suppose in fact that $ax = ay \bmod p$. As $GCD(a, p) = 1$, there is a number b such that $ba = 1 \bmod p$. Therefore $bax = bay$ so that $x = y$! □

Exercise 3.2. Compute $2^{12345} \bmod 17$

Exercise 3.3. Compute $2^{12345} \bmod 101$.

Exercise 3.4. Compute the order of 2 mod 9, 15, 21 and 35.

Can you make a guess about the general pattern?

3.1. **Euler's ϕ function.** How does Fermat's Little Theorem generalize to numbers m that are not prime? The key thing in the proof is that $\{1, 2, \cdots, p-1\}$ are coprime with p so that they have multiplicative inverses in $\mathbb{Z}_p$. It is then natural to define

$$\phi(m) = \#\{a : \ 1 \leq a \leq m-1 \text{ and } GCD(a, m) = 1\}.$$

This is *Euler's ϕ function.* We now compute its value for some m's:

(1) $\phi(p) = p-1$ for all prime numbers p. Eg. $\phi(17) = 16$.

(2) $\phi(9) = \#\{1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, 8\} = 6$

(3) $\phi(25) = \#\{1, 2, 3, 4, \cancel{5}, 6, 7, 8, 9, \cancel{10}, 11, 12, 13, 14, \cancel{15}, 16, 17, 18, 19, \cancel{20}, 21, 22, 23, 24\} = 20$

(4) $\phi(p^2) = p^2 - p$ for any prime number p. To see this, note that in the list $\{1, \cdots p^2 - 1\}$ we must erase $p, 2p, \cdots, (p-1)p$ so we have $p^2 - 1 - (p - 1) = p^2 - p$ entries.

(5) $\phi(p^n) = p^n - p^{n-1}$ for any prime number p. Explain this in detail!

(6) $\phi(6) = \#\{1, 5\} = 2$.

(7) $\phi(10) = \#\{1, 3, 7, 9\} = 4$.

(8) $\phi(14) = \#\{1, 3, 5, 9, 11, 13\} = 6$.

(9) $\phi(15) = \#\{1, 2, 4, 7, 8, 11, 13, 14\} = 8$

(10) $\phi(p \cdot q) = (p-1)(q-1)$ for any prime numbers p, q. To see this, note that in the list $\{1, \cdots, pq-1\}$ we must erase $p, 2p, \cdots, (q-1)p$ and $q, 2q, \cdots, (p-1)q$ so we have $pq - 1 - (p-1) - (q-1) = (p-1)(q-1)$ entries.

(11) $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ whenever $GCD(m, n) = 1$.

Exercise 3.5. Prove the last fact.

Exercise 3.6. Compute $\phi(1800)$.

Theorem 3.7 (Euler's Formula)**.** *If $GCD(a, m) = 1$, then*

$$a^{\phi(m)} \equiv 1 \mod m.$$

Exercise 3.8. Compute 17^{5243} mod 1800.

Exercise 3.9. Compute 2^{90} mod 91. Is 91 prime?

So if we pick a random number $0 < a < m$ and we have $a^m \neq a$ mod m, then m **is not prime.** If $a^m = a$ mod m, then m **maybe prime**. If $a^m = a$ mod m for many a's, then m **is probably prime.**

Exercise 3.10. There are some composite numbers such that $a^m = a$ mod m for all $1 \leq a \leq m - 1$! Can you find one?

3.2. **Powers mod m.** How would you compute $7^{1,000,000,000}$ mod 10403 by hand? (Or maybe with a pocket calculator.)

1) $10403 = 101 \cdot 103$ so $\phi(10403) = 10200$.

2) $10^9 = 98039 \cdot 10200 + 2200$ so $7^{1,000,000,000} = 7^{2200}$ mod 10403.

3) $7^2 = 49$, $7^4 = 49^2 = 2401$, $7^8 = 2401^2 = 1539$, $7^{16} = 1539^2 = 7040$, $7^{32} = 1708$, $7^{64} = 2401$, $7^{128} = 3733$, $7^{256} = 5672$, $7^{512} = 5508$, $7^{1024} = 2916$, $7^{2048} = 3805$. Now $2200 = 2048 + 128 + 16 + 8$ so

$$7^{2200} = 3805 \cdot 3733 \cdot 7040 \cdot 1539 = 2324 \mod 10403.$$

This was remarkably quick. It turns out that we did not need to perform $1,000,000,000$ operations. Just about $log_2(2200)$, so about 12 operations. note that in base 2, the number 2200 is 100010011000.

Exercise 3.11. Compute $2^{1,000,000,000}$ mod 35, mod 101, mod 103.

Exercise 3.12. Estimate the number of doublings needed to compute $125^{10^{100}} \bmod 101^2 \cdot 103$.

Exercise 3.13. Compute $2^{9990} \bmod 9991$ without factoring 9991. Is 9991 prime? Factor 9991.

3.3. ***k*-th roots mod m.** We wish to solve the equation

$$x^k = b \quad \mathrm{mod} m.$$

For example $x^5 = 427 \bmod 9991$.

We have that $9991 = 103 * 97$ and so $\phi(9991) = 102 * 96 = 9792$. Now, $GCD(5, 9792) = 1$ and so we can invert 5 modulo 9792. We must write $5 * u = 1 \bmod 9792$. We use the Euclidean Algorithm to get $5 * 3917 + 9792 * (-2) = 1$. Therefore

$$(x^5)^{3917} = x^{9792*2+1} = (x^{9792})^2 * x = x \quad \bmod 9991.$$

So $x = (427)^{3917} \bmod 9991$.

The general strategy to solve $x^k = b \bmod m$ where $GCD(b, m) = 1$ and $GCD(k, \phi(m)) = 1$ is exactly the same:

1. We compute $\phi(m)$. (This is easy **if we can factor** m.)
2. Write $ku = 1 + \phi(m)v$. (Use the Euclidean Algorithm.)
3. Then $x = x^{1+\phi(m)v} = x^{ku} = b^u$. (Compute b^u via the method of successive squaring.

Exercise 3.14. Solve $x^5 = 7 \bmod 35$ and $x^3 = 37 \bmod 101$.

4. RSA

The first step is to convert the alphabet to numbers. Eg. $A \to 11$, $B \to 12$, $C \to 13$, $D \to 14$, $E \to 15$, $F \to 16$, $G \to 17$, ..., $Y \to 35$, $Z \to 36$. So

$$GOODMORNING \to 1725251423252824192417$$

This code is very easy to break by frequency analysis. So we want to jumble the numbers up in a way that will look completely random (to the code breaker).

Fix p, q two very large primes (eg. 100 to 200 digits). Let $m = pq$ so that $\phi(m) = (p-1)(q-1)$. Pick k with $GCD(k, \phi(m)) = 1$.

Everyone knows m, k (they are public).

p, q (and hence $\phi(m)$) are secret.

For example, let $p = 101$, $q = 103$ so that $\phi(m) = 10200$. Pick $k = 77$.

1. Break a message up in to numbers $< m$. (Eg. 1725, 2514, 2325, 2824, 1924, 1700.)
2. Let $b_i = a_i^k \bmod m$. We compute this by repeated squaring to get the encoded message $b_1, \ldots, b_r$. This is made public/sent to the intended receiver. (Eg. $b_i = a_i^{77} \bmod 10403$ gives 4377, 9088, 1475, 2642, 3358, 3521.)

(3) To decode, solve $x^k = b_i \bmod m$. So find j with $jk = 1 \bmod \phi(m)$. Then $a_i = b_i^j \bmod m$. (Eg. $j = 8213$. Check that $kj = 1 \bmod 10200$ and that $4377^{8213} = 1725 \bmod 10403$ etc.)

This system is very easy to explain and implement on a computer. In order to decode it you must know $\phi(m)$ So you must factor m. This is very hard! Factoring a 200 digit number requires about 10^{100} computations! In contrast, it is easy to produce big primes. (We will do this later.)

Question: Couldn't we find $\phi(m)$ without factoring m and so easily break the code?

Answer: No. Since $m = pq$, if we know $\phi(m) = (p-1)(q-1) = m-p-q+1$ then we know $p+q = m-\phi(m)+1$ and so we can find the roots of $x^2-(p+q)x+m = 0$. But these are the roots of $(x-p)(x-q)$ and hence we have found p, q.

Exercise 4.1. Encode GOODMORNING using $m = 77$ (2 digits at a time). Decode $33, 71, 12, 12, 42, 53, 73, 71$.

4.1. **RSA signatures.** In practice each individual (A,B,C...) will have will have his/her secret primes p_A, q_A and will make $m_A = p_A \cdot q_A$ and k_A public.

Anyone can encrypt a message and send it to A (or B, C etc.). Just do

$$a_1, \ldots, a_r \to a_1^{k_A}, \ldots, a_r^{k_A} = b_1, \ldots, b_r.$$

We assume that $b_1, \ldots, b_r$ is public (or could be intercepted!).

Only A can decode this message since only A knows $\phi(m_A)$ so only A can solve $j_A k_A = 1 \bmod \phi(m_A)$ and then compute $a_i = b_i^{j_A} \bmod m_A$.

Suppose that A is expecting a message from B. How does A know that it really comes from the friendly B and not from the evil C?

B can attach a signature as follows:

$$BARTSIMPSON \to \alpha_1, \ldots, \alpha_s \to \alpha_1^{j_B}, \ldots, \alpha_s^{j_B} \mod m_B.$$

Only B can do this. Only B can find j_B.

Now B encodes his message with the signature appended

$$a_1, \ldots, a_r, \alpha_1^{j_B}, \ldots, \alpha_s^{j_B} \to b_1, \ldots, b_r, b_{r+1}, \ldots, b_{r+s} = a_1^{k_A}, \ldots, a_r^{k_A}, (\alpha_1^{j_B})^{k_A}, \ldots, (\alpha_s^{j_B})^{k_A}.$$

Only A can decode the message and see $a_1, \ldots, a_r, \alpha_1^{j_B}, \ldots, \alpha_s^{j_B}$. But everyone knows k_B so A can compute

$$(\alpha_1^{j_B})^{k_B}, \ldots, (\alpha_s^{j_B})^{k_B} = \alpha_1, \ldots, \alpha_s = BARTSIMPSON.$$

So A can tell that B sent the message and no one else can!

5. Counting large primes

We already know that there are infinitely many prime numbers, but how common are they?

Eg: "Half of the numbers are even."

To be more precise, if we let

$$ev(x) = \#\{even\ numbers\ n\ with\ 1 \leq n \leq x\}$$

then $ev(1) = 0$, $ev(2) = 1$, $ev(3) = 1$, $ev(4) = 2$, $ev(5) = 2$, etc. So $ev(x) = x/2$ if x is even and $ev(x) = (x-1)/2$ if x is odd. Then $ev(x)/x = 1/2$ if x is even and $ev(x)/x = 1/2 - 1/2x$ if x is odd. Then $ev(x)/x \to 1/2$ and $x \to \infty$. Eg $ev(10,000)/10,000 = 1/2$ and $ev(10001)/10,001 = 1/2 - 1/20,002 = 0.49995....$

We will now consider the function

$$\pi(x) = \#\{primes\ p\ such\ that\ p \leq x\}.$$

Exercise 5.1. Find $\pi(10)$, $\pi(25)$, $\pi(50)$, $\pi(100)$. Use a computer to find $\pi(1,000)$, $\pi(2,000)$, $\pi(4,000)$, $\pi(8,000)$, $\pi(16,000)$.

We have

x	10	25	50	100	200	500	1000	5000
$\pi(x)$	4	9	15	25	46	95	168	669
$\pi(x)/x$	.400	.360	.300	.250	.230	.190	.168	.134

It would be reasonable to guess that $\pi(x)/x \to 0$ as $x \to \infty$. This means that for any $\epsilon > 0$, we have that for big values of x the inequality $\pi(x) < \epsilon x$.

5.1. **The Prime Number Theorem.**

Theorem 5.2. *We have that $\pi(x)/(x/ln(x)) \to 1$ as $x \to \infty$, i.e.*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/ln(x)} = 1.$$

This means that for large x, the number $\pi(x)$ is very close to $x/ln(x)$.

Eg. $\pi(10^{10})/10^{10} \equiv 1/ln(10^{10}) = 1/10ln(10) = 0.0434....$ So the probability of a random number $1 \leq n \leq 10^{10}$ being prime is 4.34%.

Exercise 5.3. How many primes $\leq 10^{10}$ are there? How many primes with 10 digits? How many primes between 10^{10} and $10^{10} + 10^5$.

6. Finding large primes

We would like to produce big prime numbers (eg. with 100 digits).

We could pick a random number p with 100 digits and try and divide by all the numbers $\leq p^{1/2} \equiv (10^{100})^{1/2} = 10^{50}$. This would take way too long.

Exercise 6.1. How long would this take assuming we can perform $1,000,000,000$ divisions each second?

We will happily settle for a number which is prime with probability say 99.9999%.

6.1. **Primality testing.** How can we test if p is prime? By Fermat's little theorem, if p is prime then

$$a^p = a \mod p \text{ for all } 1 \leq a \leq p-1.$$

So if $a^p \neq a$ mod p, then p is definitely not prime. If $a^p = a$ mod p, we have some evidence that p might be prime. If $a_1^p = a_1$, $a_2^p = a_2$, ... , $a_{100}^p = a_{100}$ mod p we are tempted to conclude that p is probably prime. But what is the actual probability? Also, does this test detect all non-prime numbers?

If $n = 10$, then $2^{10} = 4$, $3^{10} = 9$, $4^{10} = 6$, $7^{10} = 9$, $8^{10} = 4$ and $9^{10} = 1$ mod 10 so we have 6 negatives (AKA witnesses) and 3 false positives (the numbers $1, 5, 6$). Therefore this test is $6/9 = 66.67\%$ effective.

Eg. $n = 935$ has 908 negatives/witnesses i.e. numbers such that $a^p \neq a$ mod p. So this test is $908/934 = 97.22\%$ accurate.

Eg. $n = 287,\ 190,\ 314$ accuracy $= 96.9\%,\ 78.9\%,\ 98.7\%$. Problem: $561 = 3 \cdot 11 \cdot 17$ satisfies $a^{561} = a$ mod 561 for all $1 \leq a \leq 561$. The test is 0% accurate.

Proof. $\phi(561) = 2 \cdot 10 \cdot 16 = 320$. It is enough to show that $a^{561} = a$ mod $3, 11, 17$.

Modulo 3: If $GCD(a, 3) = 1$, then $a^2 = 1$, so $a^{560} = (a^2)^{280} = 1^{280} = 1$.

Modulo 11: If $GCD(a, 11) = 1$, then $a^{10} = 1$, so $a^{560} = (a^{10})^5 6 = 1^{56} = 1$.

Modulo 17: If $GCD(a, 17) = 1$, then $a^{16} = 1$, so $a^{560} = (a^{16})^{10} = 1^{10} = 1$. □

Numbers with this property ($a^p = a$ mod p for all $1 \leq a \leq p-1$) are called Carmichael numbers.

Eg. 561, 1105, 1729, 2465, 2821, 6601, 8911 are all the Carmichael numbers less than $10,000$.

So maybe these numbers are very rare and this is not a problem.

Exercise 6.2. Can you show that there are infinitely many Carmichael numbers?

Notice that $22^{560} = 154 \neq 1$ mod 561, so maybe we should be testing for $a^{m-1} = 1$ mod m (not $a^m = a$ mod m). It would be even better to find a test that always works!

6.2. **The Miller Rabin test.**

Theorem 6.3. *If $p \neq 2$ is prime, then we write $p - 1 = q \cdot 2^k$ where q is odd. If $(a, p) = 1$ then either*

1) $a^q = 1$ mod p, or

2) $a^q = -1$ or $a^{2q} = -1$ or $a^{4q} = -1$ or ... or $a^{2^{k-1}q} = -1$ mod p.

Proof. We will use that fact that if p is prime, then the only numbers that square to 1 mod p are $1, -1$. Now, $a^{2^k q} = a^{p-1} = 1$ so $a^{2^{k-1}q} =$

± 1. If $a^{2^{k-1}q} = -1$ we are done, otherwise $a^{2^{k-2}q} = \pm 1$. Repeat this procedure until possibly $a^q = \pm 1$. if its $a^q = -1$ we are in case 2. Otherwise, $a^q = 1$ and we are in case 1. □

Notice that for a composite number such as 24 we may have many more square roots of 1 (eg. $1, 5, 19, 23$).

The Rabin Miller test for prime numbers works as follows: Pick n any odd integer, and write $n - 1 = q \cdot 2^k$ with q odd. If $a^q \neq 1 \bmod n$ and $a^{2^i q} \neq -1 \bmod n$ for $i = 0, 1, \ldots, k-1$, then n is composite.

Theorem 6.4. *If n is composite and odd, then at least 75% of the numbers between 1 and $n-1$ fail the Rabin Miller test. So at least 75% of such numbers are Rabin-Miller witnesses.*

So if n passes the test for 100 random numbers, then n is not prime with probability less than $0.25^{100} = 1/(2^{200}) \equiv 10^{-60}$.

Exercise 6.5. Apply the Rabin-Miller test with $a = 2$ to $n = 561$.

7. The Primitive Element Theorem

We now return to the study of powers of a number $a \bmod p$ where p is prime. By Fermat's Little Theorem, we know that for all $1 \leq a \leq p-1$ we have $a^{p-1} = 1 \bmod p$. We would now like to answer, the question: *Are there any smaller powers such that $a^e = 1 \bmod p$?*. Let $e_p(a)$ be the smallest positive number such that $a^{e_p(a)} = 1 \bmod p$. The number $e_p(a)$ is the **exponent** of $a \bmod p$.

Exercise 7.1. Find $e_p(a)$ for $1 \leq a \leq p-1$ and $p = 5, 7, 11$. Do you see a pattern?

There are two main observations, that are true for all primes:

Theorem 7.2. *Let p be any prime and $1 \leq a \leq p-1$. Then*

(1) *$e_p(a)$ divides $p-1$.*
(2) *There are exactly $\phi(p-1)$ distinct numbers $1 \leq a \leq p-1$ such that $e_p(a) = p-1$.*

Proof. For 1), if $e_p(a)$ does not divide $p-1$, then $1 \leq g = GCD(e_p(a), p-1) < e_p(a)$ and we may write $g = xe_p(a) + y(p-1)$ so that

$$a^g = a^{xe_p(a)+y(p-1)} = (a^{e_p(a)})^x \cdot (a^{p-1})^y = 1^x \cdot 1^y = 1$$

and this contradicts the fact that $e_p(a)$ is the smallest integer such that $a^e = 1 \bmod p$.

For 2) we proceed as follows: since $e_p(a)$ always divides $p-1$, we begin by counting how many a's with exponent $e < p-1$ are there? If $p - 1 = q^n$ where q is prime, then if $e_p(a) \neq p-1$, we have that $e_p(a)$ divides q^{n-1} and hence a is a root of the polynomial $x^{q^{n-1}} - 1 = 0$. There are at most q^{n-1} such roots and so there are at least $q^n - q^{n-1} > 0$ primitive roots. If $p - 1 = q_1^{n_1} \cdots q_r^{n_r}$ with $r \geq 2$, then if $e_p(a) \neq p-1$, we have that $e_p(a)$ divides $(p-1)/q_1$ or $e_p(a)$ divides $(p-1)/q_2$, so a is a root of $(x^{(p-1)/q_1}-1)(x^{(p-1)/q_2}-1)=0$. There are at most $(p-1)/q_1+(p-1)/q_2-1$ distinct roots of this equation (the root 1 is counted twice). It follows that there are at least

$$p-1-(p-1)/q_1-(p-1)/q_2+1=(p-1)(1-\frac{1}{q_1}-\frac{1}{q_2})+1>0$$

primitive roots. (We have used the fact that $q_i \geq 2$ so that $\frac{1}{q_1}+\frac{1}{q_2} \leq 1$.)

We have so far verified that there is at least one primitive root say g. So we know that

$$\{1,\dots,p-1\}=\{g,g^2,\dots,g^{p-1}\}$$

(as unordered sets). The order of g^i is $p-1$ exactly when $GCD(i,p-1)=1$ (exercise for the reader) and so we have exactly $\phi(p-1)$ primitive roots.

□

Exercise 7.3. Find an element of order 12 mod 13 (i.e. a **primitive element**). What are the other elements of order 12? Find elements of order $2,3,4,6$. Is there an element of order 5?

8. Squares modulo a prime

Exercise 8.1. Is 5 a square modulo 11? I.e. can we find a number a such that $a^2=5$ mod 11?

Exercise 8.2. Compute all squares mod 13, 17, 19, 23. Do you notice a pattern?

Theorem 8.3. *Let p be a prime, then there are $(p-1)/2$ non-zero squares mod p.*

Proof. Clearly $a^2=(-a)^2$ so there can be at most $(p-1)/2$ distinct squares. Suppose that there are less than $(p-1)/2$ squares, then there is a number say a which is the square of at least 3 different numbers, say b,c,d mod p. But then b,c,d are distinct roots of x^2-a. This is impossible! (In fact, then $x-b$, $x-c$ and $x-d$ all divide x^2-a so x^2-a is divisible by a degree 3 equation which is impossible.) □

Exercise 8.4. Show that if p is a prime and a is a root of x^2+bx+c, then a and $-(b+a)$ are the only roots of x^2+bx+c.

Exercise 8.5. Find a number m and an equation x^2+bx+c that has at least 3 solution. Conclude that x^2+bx+c has more than one factorization.

We will call the squares mod p **Quadratic Residues** or just **QR**. The non-zero numbers that are not QR will be called **Non Residues** or just **NR**.

The next observation is that if a and b are squares modulo p, then ab is a square mod p. In other words

$$QR \times QR = QR.$$

Exercise 8.6. What happens when you multiply $QR \times NR$, $NR \times NR$ or $NR \times QR$ mod 7? Experiment mod 11. Can you draw any conclusions?

Theorem 8.7. *Let p be a prime, then modulo p, we have that $QR \times QR = QR$, $QR \times NR = NR \times QR = NR$ and $NR \times NR = QR$*

Proof. The primitive root Theorem states that there is an integer g such that $g,\ g^2, \dots, g^{p-1}$ gives all numbers $1 \leq x \leq p-1$ mod p. The QR's are exactly the even powers of g and the NR are the odd powers. So, to verify that $NR \times QR = NR$ we take a non-residue of the form g^{2k+1} and a residue of the form g^{2j} and we multiply them to get $g^{2k+1}g^{2j} = g^{2(k+j)+1}$ which is not a residue as $2(k+j)+1$ is odd. □

So multiplying QR's and NR's behaves like multiplying 1 and -1. It makes sense to define the Legendre symbol of a mod p as follows: $(\frac{a}{p}) = 1$ if a is a QR mod p and $(\frac{a}{p}) = -1$ if a is a NR mod p. So, if a is a QR and b is a NR mod p, then ab is a NR mod p which can be expressed by the following equality:

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 1 \cdot (-1) = -1.$$

Exercise 8.8. Find a primitive element mod $p = 11, 13, 17$. Find all QR's mod $p = 11, 13, 17$.

Exercise 8.9. Find the sum of all QR's $1 \leq a \leq p-1$ mod $p = 11, 13, 17$. Do the same for the NR's. Do you notice a pattern?

Exercise 8.10. Compute $(\frac{-1}{p})$ for $p = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$. Do you notice a pattern?

The pattern is:

$$\left(\frac{-1}{p}\right) = 1 \text{ if} p = 1 \text{ mod } 4,$$
$$\left(\frac{-1}{p}\right) = -1 \text{ if} p = 3 \text{ mod } 4.$$

This follows immediately from
Euler's Criterion: If $p \neq 2$ is a prime, then

$$a^{(p-1)/2} = \left(\frac{a}{p}\right) \text{ mod } p.$$

Clearly, if $p = 1$ mod 4, then $p = 4k+1$ so that $(\frac{-1}{p}) = (-1)^{2k} = 1$ and if $p = 3$ mod 4, then $p = 4k+3$ so that $(\frac{-1}{p}) = (-1)^{2k+1} = -1$. It remains to prove Euler's Criterion:

Proof. If a is a QR, then $a = b^2$ so that $a^{(p-1)/2} = b^{p-1} = 1$ as required.

If a is a NR, then a is an odd power of a primitive element, i.e. $a = g^{2k+1}$ so that

$$a^{(p-1)/2} = g^{(2k+1)(p-1)/2} = (g^{p-1})^k \cdot g^{(p-1)/2} = g^{(p-1)/2}.$$

Now, $g^{p-1} = 1$ so that $g^{(p-1)/2} = \pm 1$, but since $e_p(g) = p - 1$ (i.e. $p - 1$ is the smallest power e such that $g^e = 1$), then $g^{(p-1)/2} = -1$. □

Next we would like to determine *When is* 2 *a QR mod* p*?* I.e. we would like to compute $(\frac{2}{p})$ for all odd primes.

Exercise 8.11. Determine $(\frac{2}{p})$ for all primes $3 \le p \le 47$. Do you see a pattern?

The pattern (which is hard to spot) is

$$\left(\frac{2}{p}\right) = 1 \text{ if} p = 1 \text{ or } 7 \text{ mod } 8,$$

$$\left(\frac{2}{p}\right) = -1 \text{ if} p = 3 \text{ or } 5 \text{ mod } 8.$$

Proof. We multiply the even numbers

$$2 \cdot 4 \cdot 6 \cdots (p-1) = 2^{(p-1)/2} \cdot 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}.$$

We now wish to rewrite the LHS $2 \cdot 4 \cdot 6 \cdots (p-1)$ in a different way. Consider the numbers $> (p-1)/2$ which are $\dots, (p-5),\ (p-3),\ (p-1)$ or equivalently $\dots, -5,\ -3,\ -1$. So when we multiply $2 \cdot 4 \cdot 6 \cdots (p-1)$, we are actually multiplying all the even numbers $\le (p-1)/2$ and all the odd numbers $\le (p-1)/2$ [2] with a minus sign. Therefore

$$2 \cdot 4 \cdot 6 \cdots (p-1) = (-1)^t \cdot 1 \cdot 2 \cdots \frac{p-1}{2}$$

where t is the number of odd integers $1 \le a \le (p-1)/2$. Comparing the two equations above and canceling $1 \le a \le (p-1)/2$, we get

$$2^{(p-1)/2} = (-1)^t \ mod\ p.$$

We now can easily conclude via a case by case analysis:

If $p = 1$ mod 8, then $p = 8k + 1$ so that $(p-1)/2 = 4k$ and $t = 2k$. Then $2^{(p-1)/2} = (-1)^{2k} = 1$ mod p and by Euler's Criterion, 2 is a square mod p.

If $p = 3, 5, 7$ mod 8, then $p = 8k + 3,\ 8k + 5,\ 8k + 7$ so that $(p-1)/2 = 4k + 1,\ 4k + 2,\ 4k + 3$ and hence $t = 2k + 1,\ 2k + 1,\ 2k + 2$ and hence $2^{(p-1)/2} = -1,\ -1,\ 1$ and by Euler's Criterion, 2 is a NR, NR, QR mod p. □

Exercise 8.12. Compute $(\frac{-1}{p})$ and $(\frac{2}{p})$ for $p = 101, 103, 107, 109, 113$.

Exercise 8.13. Does $x^2 + 4x + 54$ have a solution mod $97, 101, 103$?

[2] If $p - a > (p-1)/2$, then $(p+1)/2 > a$ so that $(p+1)/2 \ge a - 1$ i.e. $(p-1)/2 \ge a$.

8.1. **Quadratic reciprocity.** We would like to compute $(\frac{a}{p})$ for any integer $1 \leq a \leq p-1$. If we write $a = q_1^{n_1} \cdots q_r^{n_r}$, then we have $(\frac{a}{p}) = (\frac{q_1^{n_1}}{p}) \cdots (\frac{q_r^{n_r}}{p})$. Now if n_i is even, then $q_i^{n_i}$ is clearly a square so that $(\frac{q_i^{n_i}}{p}) = 1$. If n_i is odd, then $(\frac{q_i^{n_i}}{p}) = (\frac{q_i}{p})$. Therefore, we just need to compute

$$\left(\frac{q}{p}\right) \text{ for any primes } q, p.$$

Exercise 8.14. Make a table for $(\frac{q}{p})$ for the primes $3, 5, 7, 11, 13, 17, 19, 23, 29$. Can you see a pattern? Look at the rows and columns for $p = 5, 13, 17, 29$. Now rub these out. Is there a pattern?

The pattern is the following:

Theorem 8.15. *If $p \neq q \geq 2$ are primes, then*[3]

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \text{ if either } p = 1 \bmod 4 \text{ or } q = 1 \bmod 4,$$

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \text{ if } p \neq 1 \bmod 4 \text{ and } q \neq 1 \bmod 4.$$

Exercise 8.16. Compute $(\frac{44}{53})$, $(\frac{51}{101})$, $(\frac{91}{127})$.

We also have the **Generalized Law of Quadratic Reciprocity:**

Theorem 8.17. *Let a, b be odd numbers, then*

(1) $(\frac{-1}{b}) = 1$ *if* $b = 1$ *mod* 4 *and* $(\frac{-1}{b}) = -1$ *if* $b = 3$ *mod* 4
(2) $(\frac{2}{b}) = 1$ *if* $b = \pm 1$ *mod* 8 *and* $(\frac{2}{b}) = -1$ *if* $b = \pm 3$ *mod* 8,
(3) $(\frac{a}{b}) = (\frac{b}{a})$ if either $a = 1 \bmod 4$ or $b = 1 \bmod 4$, *and* $(\frac{a}{b}) = -(\frac{b}{a})$ if $a \neq 1 \bmod 4$ and $a \neq 1 \bmod 4$.

9. Pythagorean triples

By definition, a **Pythagorean triple** is an integer solution to the equation $a^2 + b^2 = c^2$. It yields a rectangle triangle with sides of integer length a, b, c. You are probably familiar with the Pythagorean triple $3, 4, 5$.

Exercise 9.1. Can you find any other Pythagorean triples?

Of course, $6, 8, 10$ is also a Pythagorean triple and so is $3a, 4a, 5a$ for any positive integer a. We will say that a, b, c is a **primitive Pythagorean triple** if $a^2 + b^2 = c^2$ and a, b, c have no common factors. $(5, 12, 13)$ is another such triple.

[3] Together with the rules 1) $(\frac{-1}{p}) = 1$ if $p = 1$ mod 4 and $(\frac{-1}{p}) = -1$ if $p = 3$ mod 4 and 2) $(\frac{2}{p}) = 1$ if $p = \pm 1$ mod 8 and $(\frac{2}{p}) = -1$ if $p = \pm 3$ mod 8, this is known as the **Law of Quadratic Reciprocity.**

Exercise 9.2. Can you find any other primitive Pythagorean triples? Can you show that there are infinitely many such triples? Write a program to find all such triples with $a, b \leq 100$.

We would like to find all primitive Pythagorean triples. We notice that if a and b are even, then c is even so that 2 is a common factor of a, b, c and then a, b, c is not a primitive triple. If a and b are both odd, then $a = 2x + 1$, $b = 2y + 1$ and

$$c^2 = a^2 + b^2 = 4x^2 + 4x + 1 + 4y^2 + 4y + 1 = 2 \bmod 4.$$

Now, 2 is not a square mod 4 so this is impossible. Therefore we conclude that the set a, b are not both even or odd. So, we may assume that

$$a \text{ is odd, } b \text{ is even, and } c \text{ is odd.}$$

We now consider the factorization

$$a^2 = c^2 - b^2 = (c - b)(c + b).$$

We claim that: **Both $c - b$ and $c + b$ are squares**.

Proof. First of all $g = GCD(c - b, c + b) = 1$ as otherwise g divides $c - b$ and $c + b$ so that g divides $2c = ((c - b) + (c + b))$ and g divides $2b = ((c + b) - (c - b))$. Since $c + b$ is odd, g is odd, so g divides c and b and hence g divides a (as g^2 divides $a^2 = c^2 - b^2$) so that as a, b, c have no common factor, we have $g = 1$.

So, if p is a prime number such that p divides $c + b$, then p does not divide $c - b$. Let p^t be the highest power of p dividing $c + b$, then p^t is the highest power of p dividing $a^2 = (c - b)(c + b)$. Therefore t is even and so if we write $c + b = p_1^{n_1} \cdots p_r^{n_r}$ with p_i distinct primes, we have that all the n_i are even so that $c + b$ is a square. The same reasoning also shows that $c - b$ is a square. □

So we write

$$c + b = s^2 \qquad \text{and} \qquad c - b = t^2$$

where $s > t \geq 1$ are odd integers. Therefore, we have that

Theorem 9.3. *All primitive Pythagorean triples are of the form*

$$c = \frac{s^2 + t^2}{2}, \qquad b = \frac{s^2 - t^2}{2}, \qquad \text{and} \qquad a = st$$

for some odd integers $s > t \geq 1$.

10. Which prime numbers are sums of two squares

Exercise 10.1. Find all prime numbers ≤ 47 that are sums of two squares. do you notice a pattern?

The pattern is

Theorem 10.2. *A prime number $p \neq 2$ is the sum of two squares if and only if $p = 1$ mod 4.*

Proof. **If p is the sum of two squares, then $p = 1$ mod 4:** To see this, write $p = a^2 + b^2$. As p is odd, then we may assume that a is even and b is odd. So mod 4 we have $a \in \{0, 2\}$ so that $a^2 = 0$ mod 4. Similarly $b \in \{1, 3\}$ mod 4 so that $b^2 = 1$ mod 4, so $p = 0 + 1 = 1$ mod 4.

If $p = 1$ mod 4 then p is the sum of two squares: This implication is much harder! The idea is as follows: By quadratic reciprocity, we know that $-1 = A^2$ mod p so letting $B = 1$, we have $A^2 + B^2 = 0$ mod p i.e. $A^2 + B^2 = Mp$. If $M = 1$ we are done. Otherwise we need a procedure to find new integers a, b, m such that $a^2 + b^2 = mp$ and $1 \leq m < M$. We then repeat this procedure until $m = 1$.

This is known as Fermat's Descent Procedure. This is how it works:

(1) Let p be any prime with $p = 1$ mod 4 (eg. 53), we may write $A^2 + B^2 = Mp$ with $M < p$ (eg. $13^2 + 19^2 = 10 \cdot 53$).

(2) We may pick $u = A, v = B$ mod M such that $-\frac{1}{2}M \leq u, v \leq \frac{1}{2}M$ (eg. $u = 3$, $v = -1$), then $u^2 + v^2 = A^2 + B^2 = 0$ mod M.

(3) We have $u^2 + v^2 = Mr$ and $A^2 + B^2 = Mp$ for some $1 \leq r < M$ (eg. $3^2 + (-1)^2 = 10 \cdot 1$ and $13^2 + 19^2 = 10 \cdot 53$).

Notice that $r \neq 0$ since otherwise $u^2 + v^2 = 0$ so $u = v = 0$ so $A = u = 0$ mod M and $B = v = 0$ mod M. But then M^2 divides $A^2 + B^2 = Mp$ so that M divides p. But $1 < M < p$ so that this is impossible.

Notice that $r < M$ since $r = \frac{u^2+v^2}{M} \leq \frac{(M/2)^2+(M/2)^2}{M} = \frac{M}{2} < M$.

(4) If we multiply these together, we get

$$(uA + vB)^2 + (vA - uB)^2 = (u^2 + v^2)(A^2 + B^2) = M^2 rp.$$

(5) Notice that $(uA + vB) = A^2 + B^2 = Mp = 0$ mod M and $(vA - uB) = BA - AB = 0$ mod M. So $(uA + vB)$ and $(vA - uB)$ are divisible by M. (Eg.$(uA + vB) = 39 - 19 = 20$ and $(vA - uB) = -13 - 57 = -70$.)

(6) We have therefore obtained the equation

$$\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = rp$$

with $r < M$ (eg. $2^2 + (-7)^2 = 2^2 + 7^2 = 53$). Repeating this we will get $r = 1$ as required.

□

Exercise 10.3. Use Fermat's descent procedure to write 97 as the sum of 2 squares. Do the same for $p = 881$.

11. Fermat's Last Theorem

In the 17th century Fermat stated that the equation

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

has no solutions for $n \geq 3$ and $a, b, c > 0$. Remember that for $n = 2$ this equation has infinitely many solutions and we can describe all of these. So this fact is very surprising. It also turns out to be a very deep result which was eventually proven by Wiles at the end of the 20th century. We will show the following:

Theorem 11.1. *The equation $a^n + b^n = c^n$ has no solution when n is divisible by 4 and $a, b, c > 0$.*

Proof. It is enough to show that the equation $x^4 + y^4 = z^2$ has no solution for $x, y, z > 0$. In fact if a, b, c is a solution of the original equation, then $x = a^{n/4}$, $y = b^{n/4}$ and $z = c^{n/2}$ are solutions to our new equation. The idea is once again to show that if there is a solution x, y, z, then we can find a new solution x', y', z' with $1 \leq z' < z$. We can't repeat this infinitely many times, so there was no solution to begin with!

To begin with, notice that we may assume that x, y, z have no common factor. Now, if we let $a = x^2$, $b = y^2$ and $c = z$, then a, b, c is a primitive Pythagorean triple and so we may write

$$x^2 = a = st, \qquad y^2 = b = \frac{s^2 - t^2}{2}, \qquad z = c = \frac{s^2 + t^2}{2}$$

for some odd integers s, t with no common factor. Now $st = x^2$ is an odd square so that $st = 1 \bmod 4$. It follows that either

$$s = t = 1 \bmod 4 \text{ or } s = t = -1 = 3 \bmod 4.$$

Also, we have

$$2y^2 = s^2 - t^2 = (s + t)(s - t).$$

Since s, t are odd and relatively prime, then the only common factor of $s + t$ and $s - t$ is 2. Now 4 divides $s - t$ so $s + t = 2r$ where r is an odd number. Now $2y^2 = (s - t)(s + t)$ so we have

$$s + t = 2u^2 \qquad \text{and} \qquad s - t = 4v^2$$

where $GCD(u, 2v) = 1$. Solving for s, t we get

$$s = u^2 + 2v^2 \qquad \text{and} \qquad t = u^2 - 2v^2,$$

and so from the formula $x^2 = st$ it follows that

$$x^2 = u^4 - 4v^4 \qquad \text{or} \qquad x^2 + 4v^4 = u^4.$$

We now let $A = x$, $B = 2v^2$ and $C = u^2$ so that

$$A^2 = B^2 + C^2$$

and A, B, C have no common factor i.e. A, B, C is a primitive Pythagorean triplet. Therefore, we know that there are odd relatively prime integers S, T such that

$$x = A = ST, \qquad 2v^2 = B = \frac{S^2 - T^2}{2}, \qquad u^2 = C = \frac{S^2 + T^2}{2}.$$

So we get

$$4v^2 = S^2 - T^2 = (S-T)(S+T).$$

Now $GCD(S-T, S+T) = 2$ (S, T are odd and relatively prime). So we must have

$$S + T = 2\bar{x}^2 \qquad \text{and} \qquad S - T = 2\bar{y}^2 \qquad \text{so}$$

$$S = \bar{x}^2 + \bar{y}^2 \qquad \text{and} \qquad T = \bar{x}^2 - \bar{y}^2 \qquad \text{so}$$

$$u^2 = \frac{S^2+T^2}{2} = \frac{(\bar{x}^2+\bar{y}^2)^2 + (\bar{x}^2-\bar{y}^2)^2}{2} = \bar{x}^4 + \bar{y}^4.$$

This is the new solution $(\bar{x}, \bar{y}, u)$ to the original equation $x^4 + y^4 = z^2$. We must still show that $u < z$, but this is clear from the formula

$$z = \frac{s^2+t^2}{2} = \frac{(u^2+2v^2)^2 + (u^2-2v^2)^2}{2} = u^4 + 4v^4.$$

□

12. Answers to the exercises:

Ex. (1.1) 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 87, 89, 97.

Ex. (1.2) $12 = 2^2 \cdot 3$, $123 = 3 \cdot 41$, $1234 = 2 \cdot 617$, $1235 = 5 \cdot 13 \cdot 19$, $1236 = 2^2 \cdot 3 \cdot 103$.

Ex. (1.5) 3 does not divide 71651, but it does divide 771651.

Ex. (1.6) To compute the last two digits of 273^{100} we just need to compute the last two digits of various powers of 273: $273^2 = 29$, $273^4 = 41$, $273^8 = 81$, $273^{16} = 61$, $273^{32} = 21$, $273^{64} = 41$, $273^{100} = 273^{64+32+4} = 41 * 21 * 41 = 01$. $273^{111} = 273^{64+32+16+2+1} = 41 * 21 * 61 * 29 * 73 = 57$.

Ex. (1.7) (2) $5 \cdot 9 = 1 \bmod 11$, $7 \cdot 10 = 1 \bmod 23$, $7 \cdot 29 = 1 \bmod 101$, $4^{-1} \bmod 8$ does not exist.

(3) Mod 17 we have $359 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 = -1$ so $2^8 = 1$.

(4) Mod 11 the powers of 2 are $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$ so the order is 10. The powers of 3 are $3, 9, 5, 4, 1$ so the order is 5.

The powers of 4 are $4, 5, 9, 3, 1$ so the order is 5.

The powers of 5 are $5, 3, 4, 9, 1$ so the order is 5.

The powers of 6 are $6, 3, 7, 9, 10, 5, 8, 4, 2, 1$ so the order is 10.

The powers of 7 are $7, 5, 2, 3, 10, 4, 6, 9, 8, 1$ so the order is 10.

The powers of 8 are $8, 9, 6, 4, 10, 3, 2, 5, 7, 1$ so the order is 10.

The powers of 9 are $9, 4, 3, 5, 1$ so the order is 5.

The powers of 10 are $10, 1$ so the order is 2.

(5) the squares mod 11 are: $1, 4, 9, 5, 3$ so $x^2 = 6$ has no solution mod 11 and $4^2 = 7^2 = 5$.

Ex. (2.1) $54321 = 4 \cdot 12345 + 4941$, $12345 = 2 \cdot 4941 + 2463$, $4941 = 2 \cdot 2463 + 15$, $2463 = 164 \cdot 15 + 3$, $15 = 5 \cdot 3 + 0$ so $GCD(54321, 12345) = 3$.

$45201647\%18296431 = 8608785$, $18296431\%8608785 = 1078861$, $8608785\%1078861 = 1056758$, $1078861\%1056758 = 22103$, $1056758\%22103 = 17917$ $22103\%17917 =$

$4186, 17917\%4186 = 1173, 4186\%1173 = 667, 1173\%667 = 506, 667\%506 = 161, 506\%161 = 23, 161\%23 = 0$

Ex. (2.2) $12345 = 3 \cdot 5 \cdot 823$, $54321 = 3 \cdot 19 \cdot 953$, $45201647 = 23 \cdot 1965289$ and 1965289 has no divisors ≤ 241. We would need to use a computer. $18296431 = 23 \cdot 97 \cdot 8201$ (we got lucky here).

Ex. (2.4) (1) (referring to ex. 2.1) $3 = 2463 - 164 \cdot 15 = 2463 - 164 \cdot (4941 - 2 \cdot 2463) = 329 \cdot 2463 - 164 \cdot 4941 = 329 \cdot (12345 - 2 \cdot 4941) - 164 \cdot 4941 = 329 \cdot 12345 - 822 \cdot 4941 = 329 \cdot 12345 - 822 \cdot (54321 - 4 \cdot 12345) = 3617 \cdot 12345 - 822 \cdot 54321$.

Ex. (2.5) (1) $123 = 44*2+35$, $44 = 35+9$, $35 = 9*3+8$, $9 = 8+1$ so $1 = 9-8 = 9-(35-9*3) = 4*9-35 = 4*(44-35)-35 = 4*44-5*35 = 4*44-5*(123-44*2) = 14*44-5*123$ so $14*44 = 1 \bmod 123$.

Ex. (2.6) $......abcd * 17 = 1 + X * 10^{100} = ...0001$. So $17d = 1 \bmod 10$ i.e. $d = 3$,

$c3 * 17 = 1 \bmod 100$ i.e. $c * 170 = 1 - 51 = -50 = 50 \bmod 100$ so that $c * 7 = 5$, mod 10 so that $c = 5$,

$b53 * 17 = 1 \bmod 1000$ i.e. $b * 1700 = 1 - 901 = 100 \bmod 1000$ i.e. $b * 7 = 1$, mod 10 so $b = 3$

$a353 * 17 = 1 \bmod 10000$ i.e. $a * 17000 = 1 - 6001 = 4000 \bmod 10000$ so $a * 7 = 4 \bmod 10$ so $a = 2$.

Ex. (2.7) $10^{10} = 103 * 97087378 + 66$, $103 = 66 + 37$, $66 = 37 + 29$, $37 = 29 + 8$, $29 = 8 * 3 + 5$, $8 = 5 + 3$, $5 = 3 + 2$, $3 = 2 + 1$. So $1 = 3 - 2 = 3 - (5 - 3) = 3 * 2 - 5 = (8 - 5) * 2 - 5 = 8 * 2 - 5 * 3 = 8 * 2 - (29 - 8 * 3) * 3 = 8 * 11 - 29 * 3 = (37 - 29) * 11 - 29 * 3 = 37 * 11 - 29 * 14 = 37 * 11 - (66 - 37) * 14 = 37 * 25 - 66 * 14 = (103 - 66) * 25 - 66 * 14 = 103 * 25 - 66 * 39 = 103 * 25 - (10^{10} - 103 * 97087378) * 39 = 103 * 3786407767 - 10^{10} * 39$. So $103^{-1} = 3786407767 \bmod 10^{10}$ so $SSN = 3536767732 * 3786407767 = 519774444 \bmod 10^{10}$

Ex. (3.2) $2^2 = 4$, $2^4 = (2^2)^2 = 4^2 = 16 = -1$, $2^8 = (2^4)^2 = (-1)^2 = 1$. Since $12345 = 8 \cdot 1543 + 1$, we have

$$2^{12345} = (2^8)^{1543} \cdot 2 = 1^{1543} \cdot 2 = 2.$$

Ex. (3.3) $2^2 = 4$, $2^4 = 16$, $2^8 = 256 = 54$, $2^{16} = 54^2 = 2916 = 88$, $2^{32} = 88^2 = 7744 = 68$. So

$$2^{12345} = (2^{100})^{123} \cdot 2^{45} = 1^{123} \cdot 2^{32+8+4+1} = 68 \cdot 54 \cdot 16 \cdot 2 = 41.$$

Ex. (3.4) Mod 9: $2^3 = -1$, $2^6 = 1$.
Mod 15: $2^4 = 16 = -1$, $2^8 = 1$. The order is 8.
Mod 21: $2^5 = 32 = 11$, $2^6 = 22 = 1$. The order is 6.
Mod 35: $2^6 = 64 = 29$, $2^7 = 58 = 23$, $2^8 = 46 = 11$, $2^9 = 22$, $2^{10} = 44 = 9$, $2^{11} = 18$, $2^{12} = 36 = 1$. The order is 12.

Ex. (3.6) 480.

Ex. (3.8) 17.

Ex. (3.9) $2^{90} = 64 \neq 1 \bmod 91$. 91 is not prime!

Ex. (3.11) Mod 35, we have $\phi(35) = 4 * 6 = 24$ so $10^9\%24 = 16$ and $2^{10^9} = 2^{16}$. Now $2^4 = 16$, $2^8 = 16^2 = 256 = 11$, $2^{16} = 11^2 = 121 = 16$.

Mod 101: $\phi(101) = 100$ so that $2^{10^9} = (2^{100})^{10^7} = 1^{10^7} = 1$.

Mod 103: $\phi(103) = 102$, $10^9\%102 = 58$. $2^4 = 16$, $2^8 = 256 = 50$, $2^{16} = 2500 = 28$, $2^{32} = 28^2 = 784 = 63$, $2^{58} = 2^{32+16+8+2} = 63 * 26 * 50 * 4 = 25$.

Ex. (3.12) $\phi(101^2 \cdot 103) \equiv 1,000,000$ and $log_2(10^6) \equiv 20$ so about 20 doublings.

Ex. (3.13) $2^{9990} = 4599 \bmod 9991$.

Ex. (3.14) Mod 35: $\phi(35) = 24$, $5 * 5 = 1 \bmod 24$ so $x = (x^5)^5 = 7^5 = 7 \bmod 35$.

Mod 101: $\phi(101) = 100$ and $3 * 67 = 201 = 1 \bmod 100$ so $x = (x^3)^{67} = 37^{67} \bmod 101$. Now $37^2 = 56$, $37^4 = 5$, $37^8 = 25$, $37^{16} = 19$, $37^{32} = 58$, $37^{64} = 31$. So $37^{67} = 31 * 56 * 37 = 97$.

Ex. (4.1) 52, 53,53,42,23,53,63,73,68,73,52; WELLDONE (note that $\phi(77) = 60$ and $7 * 103 = 721 = 1 \bmod 60$).

Ex. (5.3) $\pi(10^{10}) \equiv 434,294,482$; $\pi(10^{10}) - \pi(10^9) \equiv 434,294,482 - 48,254,942 = 386,039,540$; $\pi(10^{10} + 10^5) - \pi(10^{10}) = 4,514$

Ex. (6.1) $10^{41}s = 2.77 * 10^{37}hrs = 3.16 * 10^{33}$ years.

Ex. (7.1) $n-1 = 560 = 35 \cdot 2^4$. $2^{35} = 263 \bmod 561$. $2^{70} = 263^2 = 166 \bmod 561$. $2^{140} = 166^2 = 67 \bmod 561$. $2^{280} = 67^2 = 1 \bmod 561$ and $2^{560} = 1^2 = 1 \bmod 561$. So 561 failed the Rabin-Miller test, therefore it can not be prime. 2 is a Rabin-Miller witness for the number 561.

Ex. (7.3) $2^4 = 3$ and $2^3 = 8 \bmod 13$, so the order of 2 is 12. The other elements of order 12 are 2^5, 2^7, 2^11. 2^2 has order 6, 2^3 has order 4, 2^4 has order 3 and 2^6 has order 2.

Ex. (8.1) We square all the residues mod 11 and we get $0 = 0^2$, $1 = 1^2 = 10^2$, $4 = 2^2 = 9^2$, $9 = 3^2 = 8^2$, $5 = 4^2 = 7^2$ and $3 = 5^2 = 6^2$ mod 11. So the answer is yes.

Ex. (8.2) Mod 13: $1, 4, 9, 3, 12, 10$.

Mod 17: $1, 4, 9, 16, 8, 2, 15, 13$.

Mod 19: $1, 4, 9, 16, 6, 17, 11, 7, 5$

Mod 23: $1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6$.

Ex. (8.4) $(x - a)(x + b + a) = x^2 + b * x - a(b + a)$ so we must show that $c = -a(b + a)$ but this is clear as a is a root of $x^2 + b * x + c$ so $a^2 + ab + c = 0$. If z is a third root of $x^2 + b * x + c \bmod p$, then $(z - a)(z + b + a) = 0$ so that p divides $(z - a)$ or it divides $(z + b + a)$, but then $z = a \bmod p$ or $z = -b - a \bmod p$. So these are the only two roots.

Ex. (8.5) $2, 4, 8, 10$ are roots of $x^2 = 4 \bmod 12$ so $x^2 - 4 = (x - 2)(x - 10) = (x - 4)(x - 8)$.

Ex. (8.6) QR=1, 4, 2; NR = 3, 5, 6 so QR * NR =NR * QR =3, 5, 6 =NR and NR * NR = 1, 4, 2 = QR.

Ex. (8.8) Mod 11: 2; QR= $2^0 = 1$, $2^2 = 4$, $2^4 = 5$, $2^6 = 9$, $2^8 = 3$.

Mod 13: 2; QR= $2^0 = 1$, $2^2 = 4$, $2^4 = 3$, $2^6 = 12$, $2^8 = 9$, $2^{10} = 10$.

Mod 17: 3; QR$=3^0 = 1$, $3^2 = 9$, $3^4 = 13$, $3^6 = 15$, $3^8 = 16$, $3^{10} = 8$, $3^{12} = 4$, $3^{14} = 2$.

Ex. (8.9) Mod 11: $1{+}4{+}5{+}9{+}3 = 22$; Mod 13: $1{+}4{+}3{+}12{+}9{+}10 = 39$ Mod 17: $1+9+13+15+16+8+4+2 = 68$. They are all 0 mod p.

Ex. (8.10) $(\frac{-1}{3}) = -1$, $(\frac{-1}{5}) = 1$, $(\frac{-1}{7}) = -1$, $(\frac{-1}{11}) = -1$, $(\frac{-1}{,}13) = 1$, $(\frac{-1}{17}) = 1$, $(\frac{-1}{19}) = -1$ $(\frac{-1}{,}23) = -1$, $(\frac{-1}{29}) = 1$, $(\frac{-1}{31}) = -1$.

Ex. (8.11) $(\frac{2}{3}) = -1$, $(\frac{2}{5}) = -1$, $(\frac{2}{7}) = 1$, $(\frac{2}{11}) = -1$, $(\frac{2}{13}) = -1$, $(\frac{2}{17}) = 1$, $(\frac{2}{19}) = -1$, $(\frac{2}{23}) = 1$, $(\frac{2}{29}) = -1$, $(\frac{2}{31}) = 1$, $(\frac{2}{37}) = -1$, $(\frac{2}{41}) = 1$, $(\frac{2}{43}) = -1$, $(\frac{2}{47}) = 1$.

Ex. (8.12) $(\frac{-1}{p}) = 1, -1, -1, 1, 1$ and $(\frac{2}{p}) = -1, 1, -1, -1, 1$.

Ex. (8.13) $x^2 + 4x + 54 = (x + 2)^2 + 50$ so is $-50 = -1 * 2 * 5^2$ a square mod p? Equivalently is $-1 * 2$ a square mod p?

Mod 97: $(\frac{-1}{97}) = -1$ and $(\frac{2}{97}) = 1$ so no.

Mod 101: $1 * (-1) = -1$ so no.

Mod 103 $(-1) * 1$ so no.

Ex. (8.16) $(\frac{44}{53}) = (\frac{11}{53}) = (\frac{53}{11}) = (\frac{9}{11}) = 1$; $(\frac{51}{101}) = (\frac{101}{51}) = (\frac{49}{51}) = 1$; $(\frac{91}{127}) = (\frac{127}{91}) = -(\frac{36}{91}) = -1$.

Ex.(10.1) $2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 5^2$, $29 = 2^2 + 5^2$, $37 = 1^2 + 6^2$, $41 = 4^2 + 5^2$.

Ex. (10.3) $A = 1$, $B = 22$ so $1^2 + 22^2 = 5 * 97$ so $M = 5$, $u = 1$, $v = 2$ so $(uA + vB)/M = 9$ and $(vA - uB)/M = -4$, so $97 = 4^2 + 9^2$.