4. Number Theory

Terence Sim

God made the integers, all else is the work of man.

Leopold Kronecker,
1823 — 1891

Reading

Sections 4.1 — 4.7 of Epp

4.1. Recap

Definition 1.3.1 (Divisibility)

If n and d are integers and $d \neq 0$ then

n is **divisible by** d if, and only if, n equals d times some integer.

Instead of "n is divisible by d," we can say that

n **is a multiple of** d, or
d **is a factor of** n, or
d **is a divisor of** n, or
d **divides** n.

The notation $\mathbf{d \mid n}$ is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

Reminder: No division is actually performed when we say: $d \mid n$.

Theorem 4.1.1

$\forall a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $\forall x, y \in \mathbb{Z}, a \mid (bx + cy)$

That is, if a divides both b and c, then a divides their linear combination.

Note that this statement was in Slide 29 of `proofs-handout.pdf`, and also Q7. of Tutorial 1.

Since it is useful, we make it a theorem.

Proof.

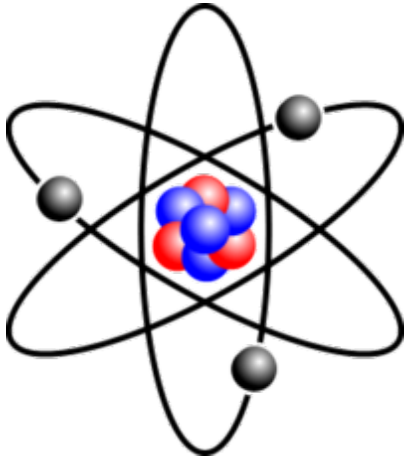
1. For any $a, b, c \in \mathbb{Z}$:
2. If $a \mid b$ and $a \mid c$:
3. Let $k \in \mathbb{Z}$ such that $b = ak$. (by definition of divisibility)
4. Let $m \in \mathbb{Z}$ such that $c = am$. (by definition of divisibility)
5. For any $x, y \in \mathbb{Z}$:
6. $bx + cy = (ak)x + (am)y = a(kx + my)$. (by basic algebra)
7. Note that $kx + my \in \mathbb{Z}$. (by closure of addition and multiplication over integers)
8. Thus $a \mid bx + cy$. (by definition of divisibility) ■

4.2. Primes

Prime numbers are to integers what atoms are to materials.

They are the indivisible building blocks of integers.

We will learn some key properties and see some applications of prime numbers.



Definition 4.2.1 (Prime number)

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

$$n \text{ is prime} \Leftrightarrow \forall \text{ positive integers } r \text{ and } s, \text{ if } n = rs \text{ then either } r = 1 \text{ and } s = n \text{ or } r = n \text{ and } s = 1.$$

$$n \text{ is composite} \Leftrightarrow \exists \text{ positive integers } r \text{ and } s \text{ such that } n = rs \text{ and } 1 < r < n \text{ and } 1 < s < n.$$

- 1 is neither prime nor composite.
- The first few primes are: $2, 3, 5, 7, 11, 13, 17, 19$.
- The first few composites are: $4, 6, 8, 9, 10, 12, 14, 15$.

Every integer $n > 1$ is either prime or composite.

To see this, consider all positive pairs r, s such that $n = rs$. There is always the trivial pairs $r = n, s = 1$, and $r = 1, s = n$. Note that they satisfy $1 \leq r, s \leq n$. But if these are the *only* pairs, then n is prime by definition.

Otherwise, there exists a positive pair r, s such that $n = rs$ and $1 < r, s < n$. And thus n is composite by definition.

4.2.1. Prime properties

Primes have interesting properties, some of which we will now study. We begin with the property that if one prime divides another, then they must be equal.

Proposition 4.2.2

For any two primes p and p', if $p \mid p'$ then $p = p'$.

Note that this property does not hold for composites, e.g. $4 \mid 8$ but $4 \neq 8$.

Proof:

1. For any primes p and p':
2. If $p \mid p'$:
3. Let $k \in \mathbb{Z}$ such that $p' = pk$, by definition of divisibility.
4. Then $p = 1$ or $p = p'$, since p' is prime.
5. Also, $p > 1$, since p is prime.
6. Therefore $p = p'$. ■

The next property of primes sets the stage for the important fact that prime numbers do not end; ever larger primes exist.

Proposition 4.7.3 (Epp)

For any $a \in \mathbb{Z}$ and any prime p, if $p \mid a$ then $p \nmid (a+1)$.

Proof: (by Contradiction)

1. Suppose not. Then there exists $a \in \mathbb{Z}$ and prime p such that $p \mid a$ and $p \mid (a+1)$.
2. Then $p \mid a(-1) + (a+1)(1)$, by Theorem 4.1.1.
3. Then $p \mid 1$, by basic algebra.
4. By Theorem 4.3.1 (Epp), this implies $p \leq 1$, which contradicts the fact that $p > 1$.
5. Thus by the Contradiction Rule, the statement is true. ■

The statement to be proven takes the form:

$$S = \forall x(\forall y(P(x,y) \rightarrow Q(x,y)))$$

Thus, its negation is:

$$\begin{aligned}
\sim S &\equiv \sim (\forall x(\forall y(P(x,y) \rightarrow Q(x,y)))) \\
&\equiv \exists x \sim (\forall y(P(x,y) \rightarrow Q(x,y))) \\
&\equiv \exists x(\exists y \sim (P(x,y) \rightarrow Q(x,y))) \\
&\equiv \exists x(\exists y \sim (\sim P(x,y) \vee Q(x,y))) \\
&\equiv \exists x(\exists y(\sim (\sim P(x,y)) \wedge \sim Q(x,y))) \\
&\equiv \exists x(\exists y(P(x,y) \wedge \sim Q(x,y)))
\end{aligned}$$

The last line is the form used in Step 1 of the proof.

Theorem 4.7.4 (Epp): Infinitude of Primes.

The set of primes is infinite.

Proof: (by Contradiction)

1. Suppose the set of primes is finite: a total of k primes.
2. Then we may list all the primes: $p_1, p_2, p_3, \ldots, p_k$
3. Let N be the product of all primes plus 1: $N = p_1 p_2 p_3 \cdots p_k + 1$.
4. Clearly, $N > 1$, and thus by Theorem 4.3.4 (Epp), there exists a prime q such that $q \mid N$.

...

proof cont'd

5. Now $q \mid p_1 p_2 p_3 \cdots p_k$ because q is one of the factors in the product.
6. Then by Proposition 4.7.3 (Epp), $q \nmid N$, which contradicts Line 4 which says $q \mid N$.
7. Thus by the Contradiction Rule, the statement is true. ■

- This proof shows that if you form the product of all primes up to some point and add 1, the result, N, is divisible by a prime not in the list.
- Note that this does not mean that N is prime. As an exercise, try to find an N constructed in this way that is not prime.

So now we know that primes do not end. Ever larger primes can always be found.

But they seem fewer and fewer as we examine larger integers.

> For example, there are 4 primes under 10, but 25 primes under 100. To get the thousandth prime, you need to search up to about 8000; to get the millionth prime, your search goes to about 15.5 million.

The Prime Number Theorem tells us that the number of primes less than or equal to integer x is approximately $x/\log(x)$.

Watch this video: `http://tinyurl.com/nrwal9x`

Theorem 4.2.3

If p is a prime and $x_1, x_2, \ldots, x_n$ are any integers such that:

$$p \mid x_1 x_2 \ldots x_n,$$

then $p \mid x_i$, for some x_i $(1 \leq i \leq n)$.

For example, consider $2 \times 3 \times 6 = 36$:

Clearly, 3 is prime, and $3 \mid 36$ and $3 \mid 6$.

However, the theorem does not hold for composites, e.g. 4 is composite and $4 \mid 36$. But $4 \nmid 2$, and $4 \nmid 3$ and $4 \nmid 6$.

This theorem shows that a prime factor of a product must be completely "inside" one of the factors of the product. The prime cannot be "split" into several of the factors.

Theorem 4.3.5 (Epp): Unique Prime Factorization

Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

That is, every positive integer greater than 1 can be uniquely factorized into a product of prime numbers.

This is also called *The Fundamental Theorem of Arithmetic*.

It is standard practice to sort the primes from smallest to largest. Examples:

$$24 = 2 \times 2 \times 2 \times 3 = 2^3 \cdot 3.$$

$$90 = 2 \times 3 \times 3 \times 5 = 2 \cdot 3^2 \cdot 5.$$

Suppose m is an integer such that

$$8 \cdot 7 \cdot 6 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14$$

Does $17 \mid m$?

Since 17 is a prime factor of the right hand side, it must also divide the product on the left hand side.

Then by Theorem 4.2.3, 17 must divide one of the factors on the left hand side. This must be m because the other factors are not divisible by 17.

Thus, $17 \mid m$.

4.2.2. An application

Suppose you wish to send a message consisting of two positive integers m, n to a friend. Unfortunately, the Send device can only send a single integer, however large, but not two. The Receive device is likewise limited to receiving only a single integer.

You thus need a way to encode, i.e. convert, your m, n into s, as well as a way to decode. This is shown in the diagram below.

How would you encode?

1. Suppose you encode m, n by inserting a 0 between their decimal representations, e.g.

   1234 and 768 gets encoded to 12340768

   Clearly, this won't work if m or n contains 0.
2. Suppose you try $s = m + n$. This doesn't work either. Why?
3. Next, you try $s = 1000m + n$. Will this work?
4. Clearly, $s = mn$ also doesn't work.
5. Luckily, you remember CS1231, so you try $s = 2^m 3^n$.

   This works because the prime factorization of s guarantees that we can get back m and n uniquely!

Question: how would you handle negative m and n?

Python code for encode and decode:

```
def encode(m, n):
    return 2**m * 3**n

def decode(s):
    # Repeatedly divide s by 2, and count number of times
    # this can be done. Do the same for 3.

    m = 0
    while isEven(s):
        s = s / 2
        m = m + 1

    n = 0
    while isColorful(s):
        s = s / 3
        n = n + 1

    return m,n
```

Python code cont'd

```
def isEven(x):
    # x is even if its remainder is 0
    # when divided by 2
    return x % 2 == 0

def isColorful(x):
    # x is colorful if its remainder is 0
    # when divided by 3
    return x % 3 == 0
```

4.2.3. Primality test

This is a test to see if an integer n is prime.

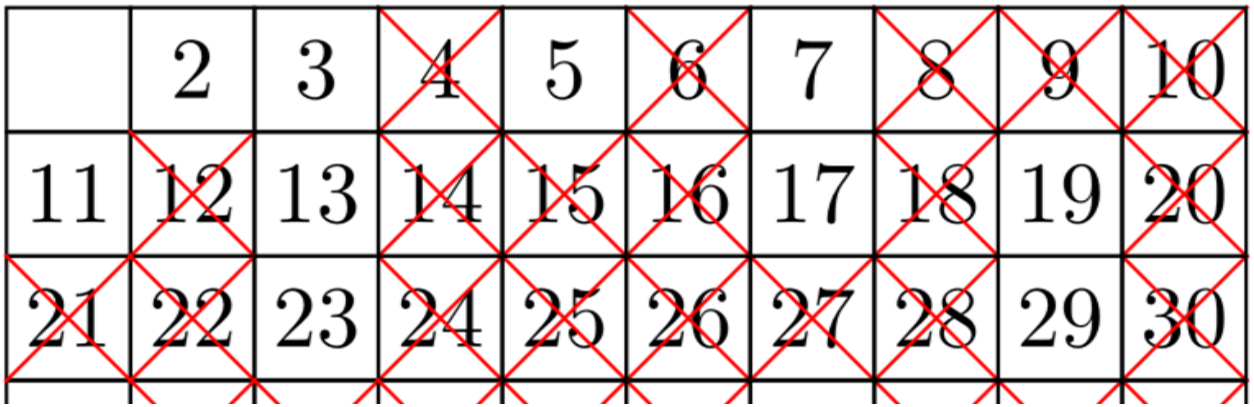
The most straightforward method is Trial Division, i.e. test if n is divisible by all integers k between 2 and $\sqrt{n}$ (rounded up). If n is not divisible by all such k, then n is prime, otherwise, composite.

This test is easy to code, but is slow. It can be sped up using only k which are primes, but this requires a list of such primes to begin with.

The side benefit of Trial Division is that you also get all the factors of n, if n is composite.

Of course, one way to check if a number n is prime is to see if n can be found in a list, L, of primes. To generate L, an ancient method called the Sieve of Eratosthenes may be used:

1. Start by listing all integers greater than 1. Call this list C. Also, let L be an empty list.
2. Take the first number $p = 2$ in C, and add it to L. This is the first prime.
3. In C, cross out all multiples of p.
4. Let p be the next uncrossed number in C. This is the next prime. Add it to L, and repeat from Step 3.



A more sophisticated method is the Miller-Rabin probabilistic test. More correctly, it tests for compositeness.

An integer, suspected of being a composite, is "put on trial". The Judge (algorithm) randomly picks a person (another integer) and asks a series of questions concerning the Suspect.

If the person provides sufficient evidence, the person is then called a *Witness* and the Suspect is guilty of being a Composite, and the trial ends.

If not, then another random person is picked, and the trial is repeated several times. If no Witness emerges, then the Suspect is probably a Prime.

Thus the Miller-Rabin test can make errors: a composite may be passed off as a prime. Such a composite is called a *pseudoprime*. But the probability of error can be made small.

Still, in some applications, having a non-zero probability of getting a pseudoprime is unacceptable, e.g. in Cryptography. In this case, other primality tests are needed.

Furthermore, the Miller-Rabin test does not tell you the factors of the composite; it merely tells you if the integer is composite or probably prime.

Primality testing is still an active research area.

4.2.4. Open Questions

There are several Open Questions concerning prime numbers, i.e. questions for which answers are still lacking or unproven. Proving any of these will earn you a Ph.D. immediately, and land you a professorship at a prestigious university.

We mention two Open Questions:

Goldbach's Conjecture: Every even integer greater than 2 can be written as a sum of two primes.

Examples: $4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 3 + 5.$

This Conjecture has been shown to be true for integers up to 4×10^{18}, but this is still far from proving it for *all* even integers.

Twin Primes Conjecture: There are infinitely many primes p such that $p + 2$ is also a prime.

Examples: $(3, 5)$, $(11, 13)$, $(41, 43)$.

Twin primes are primes separated by a gap of 2. In 2013, Yitang "Tom" Zhang, a hitherto unknown mathematician, rocked the world of mathematics by making in a big leap in proving the Twin Primes Conjecture.

He proved that there are infinitely many primes whose gap is at most 70 million. Although this gap is much larger than 2, Zhang's work sparked a revival in research in this area. A year later, through the efforts of many researchers, this gap is now reduced to 246.

Zhang, who had struggled to secure an academic job since getting his Ph.D. in 1991, and at one time even worked as a restaurant delivery worker, quickly got promoted to Full Professor.

Watch this video: `http://tinyurl.com/mv2xuq7`

4. Number Theory (Part 2)

Terence Sim

Mathematics is the queen of the sciences and number theory is the queen of mathematics.

Carl Friedrich Gauss,
1777— 1855

Reading

Sections 4.8, 5.2 — 5.4 of Epp.

4.3. Well Ordering Principle

Definition 4.3.1 (Lower Bound)

An integer b is said to be a lower bound for a set $X \subseteq \mathbb{Z}$ if $b \leq x$ for all $x \in X$.

Note that this definition does not require b to be a member of X.

Moreover, there may be more than one lower bound (ie. the lower bound is not unique).

Examples: Does each of the following sets have a lower bound?

- $A = \{x \in \mathbb{Z} \mid x^2 \leq 38\}$.
- $B = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 3\}$.
- $C = \{x \in \mathbb{Z} \mid x^2 \leq 100x\}$.

Answer:

- We may list all the elements of the set. $A = \{-6, -5, \ldots, 5, 6\}$. Thus, any integer less than or equal to -6 is a lower bound.
- There is no lower bound. To see this, suppose not; suppose the lower bound is some integer c. Then one of $c-1, c-2, c-3$ must be divisible by 3. But all of them are less than c, contradicting the fact that c is a lower bound.
- If $x^2 \leq 100x$ then $x(x-100) \leq 0$, by basic algebra. Thus C is the set of integers x such that $0 \leq x \leq 100$. Thus any integer $m \leq 0$ is a lower bound.

Theorem 4.3.2 (Well Ordering Principle)

If a non-empty set $S \subseteq \mathbb{Z}$ has a lower bound, then S has a least element.

Proof omitted.[1]

This was stated in a slightly different (in terms of a predicate $P(n)$), and more formal, way in the notes `induction.pdf`. Both forms are equivalent, by defining S to be the truth set of the predicate P. The proof that Induction may be derived from Well Ordering, and vice versa, was also shown in the notes.

[1] Text in green are corrections of errors.

Examples: Does each set below have a least element? If so, what is it? If not, explain why there is no violation of the Well Ordering Principle.

- The set of all positive real numbers.
- The set of all non-negative integers n such that $n^2 < n$.
- The set of all non-negative integers of the form $46 - 7k$, where k is any integer.

Answer:

- There is no least (smallest) positive real number. To see this, suppose $x \in \mathbb{R}^+$, then $x/2 \in \mathbb{R}^+$ and $x/2 < x$. There is no violation of the Well Ordering Principle because the principle concerns only sets of integers, not real numbers.
- This set is empty! Thus there is no least element, and no violation of the Well Ordering Principle.
- Now, $46 - 7k \geq 0$ implies $7k \leq 46$, which means $k \leq 6.57$. When $k = 6$, $46 - 7(6) = 4$, which is therefore the least element.

Proposition 4.3.3 (Uniqueness of least element)

If a set S of integers has a least element, then the least element is unique.

The usual way to prove the uniqueness of a solution is to say that if A and B are both solutions, then $A = B$.

First let's define what it means to be a least element:

The least element x of a set S is one that satisfies:

(i) $x \in S$.

(ii) $\forall y \in S,\ x \leq y$.

Proof:

1. Suppose x and z are two least elements in S:
2. Then $\forall y \in S$, $x \leq y$, by definition of least element.
3. Since $z \in S$, this means $x \leq z$ [Universal instantiation].
4. Also, since z is a least element, then $\forall w \in S$, $z \leq w$, by definition of least element.
5. And since $x \in S$, this means $z \leq x$ [Universal instantiation].
6. Now, $(x \leq z) \wedge (z \leq x)$ simplifies to $x = z$, by the distributive and identity laws of logical equivalences.
7. Thus the least element is unique. ■

Well Ordering also states the existence of the greatest (maximum) element too:

Theorem 4.3.2 Well Ordering 2

If a non-empty set $S \subseteq \mathbb{Z}$ has an upper bound, then S has a greatest element.

The definition for upper bound is analogous to that for lower bound, ie. it is an integer that is more than or equal to all elements in the set. The upper bound need not be in the set, and is not unique.

Proposition 4.3.4 (Uniqueness of greatest element)

If a set S of integers has a greatest element, then the greatest element is unique.

The proof is similar to that for Proposition 4.3.3.

4.4. Quotient-Remainder Theorem

Theorem 4.4.1 (Quotient-Remainder Theorem)

Given any integer a and any positive integer b, there exist unique integers q and r such that:

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

The integer q is called the quotient, while r is called the remainder.

Note the limits on r: r lies in the range $0, 1, 2, \ldots, b - 1$.

Proof:

1. Let R be the set of "remainders":
   $$R = \{x \in \mathbb{N} \mid a = by + x \text{ for some } y \in \mathbb{Z}\}.$$
2. (Claim: R is not empty.)
3. If $a \geq 0$:
4. Then $a = b \cdot 0 + a \geq 0$, and thus $a \in R$.
5. Else $a < 0$:
6. Then $a - ab = a(1 - b) \geq 0$ [because $a < 0$ and $(1 - b) \leq 0$, so their product ≥ 0.]
7. Thus $(a - ab) \in R$ by definition of R.
8. In either case, R has at least one element.
9. Thus R is a non-empty subset of integers, and there exists a least element $r \in R$, by the Well Ordering Principle.

...

proof cont'd

10. Then there exists $q \in \mathbb{Z}$ such that $a = bq + r$, since $r \in R$.
11. Suppose $r \geq b$:
12. Re-write: $a = b(q + 1) + (r - b)$ by basic algebra.
13. Thus $(r - b) \in R$, by definition of R.
14. But $r - b < r$, contradicting the fact the r is the least element.
15. Thus $0 \leq r < b$.
16. Furthermore, r, as the least element, is unique by Proposition 4.3.3.
17. And since $a = bq + r$, this means q is unique also. ■

Line 17 could be more rigorously justified.

Note that neither the theorem nor the proof says how to calculate q and r from a, b. They merely say q, r exist.

Examples: Find the quotient and remainder for each of the following.

- $a = 54, b = 4$
- $a = -54, b = 4$
- $a = 54, b = 70$

- $54 = 4 \times 13 + 2$, so $q = 13, r = 2$.
- $-54 = 4 \times (-14) + 2$, so $q = -14, r = 2$.
- $54 = 70 \times 0 + 54$, so $q = 0, r = 54$.

Most programming lanauges have operations called `div` and `mod`, which compute the quotient and remainder, respectively, for positive integers a, b.

In C/C++ and Java the integer division "/" computes the quotient, while "%" computes the remainder. However, these do not give the correct answer if a is negative, e.g. C gives $q = -13, r = -2$ when $a = -54, b = 4$. Thus some caution is advised.

Division Algorithm

```
def division(a, b):
    #assumes a>=0, b > 0
    q = 0
    r = a

    while r >= b:
        r = r - b
        q = q + 1

    return q,r
```

This algorithm computes the quotient and remainder for non-negative integer a and positive integer b. The key idea is to repeatedly subtract b from a until the result is less than b, and to count the number of subtractions.

4.4.1. Representation of Integers

The Quotient-Remainder Theorem provides the basis for writing an integer n as a sequence of digits in a base b.

For example, our usual way of writing the number $n = 3 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$ is: 334. This is in decimal (base 10) because it uses powers of 10. The same number n could be represented using a different base. More generally, given any positive integer n and base b, we may repeatedly apply the Quotient-Remainder Theorem to get:

$$\begin{aligned} n &= bq_0 + r_0 \\ q_0 &= bq_1 + r_1 \\ q_1 &= bq_2 + r_2 \\ &\vdots \\ q_{m-1} &= bq_m + r_m \end{aligned}$$

- Each remainder r_i is one of the integers $0, 1, \ldots, b-1$, and the process stops when $q_m = 0$.
- By eliminating the quotients q_i, we get:

$$n = r_m b^m + r_{m-1} b^{m-1} + \ldots + r_1 b + r_0$$

which may be written more compactly as:

$$n = \sum_{i=0}^{m} r_i b^i$$

- In turn, we may write n more compactly in base b as a sequence of the digits r_i. That is:

$$n = (r_m r_{m-1} \ldots r_1 r_0)_b$$

This positional notation is convenient. When $b = 10$ we usually omit it, which gives us our usual decimal representation for integers.

Note that the summation notation $\sum_{i=a}^{b} f(i)$ is shorthand for:

$$f(a) + f(a+1) + f(a+2) + \ldots + f(b-1) + f(b)$$

The index i increments by 1 starting from the lower limit a and ending at the upper limit b. It is assumed $b \geq a$. If $b < a$, then the sum is empty, which by default equals 0.

Likewise, a product of terms $f(a) \times f(a+1) \times \ldots \times f(b-1) \times f(b)$ is more compactly written as:

$$\prod_{i=a}^{b} f(i)$$

Again, it is assumed $b \geq a$. And if $b < a$ then the product is empty, which by default equals 1.

Example: Express $(109)_{10}$ in base 2.

Answer: Dividing repeatedly by 2 we obtain:

$$\begin{aligned} 109 &= 2 \times 54 + 1 \\ 54 &= 2 \times 27 + 0 \\ 27 &= 2 \times 13 + 1 \\ 13 &= 2 \times 6 + 1 \\ 6 &= 2 \times 3 + 0 \\ 3 &= 2 \times 1 + 1 \\ 1 &= 2 \times 0 + 1 \end{aligned}$$

Hence, by reading the remainders from bottom up, $(109)_{10} = (1101101)_2$. Base 2 (or binary) representation is especially useful for computers to manipulate.

Another useful base for computer manipulation is 16, called hexadecimal.

Here, we need new symbols to represent the decimal digits $10, 11, \ldots, 15$ in base 16. The usual convention is:

$$\text{A=10, B=11, C=12, D=13, E=14, F=15}$$

For the previous example of $(109)_{10}$, we may repeatedly divide by 16 to get: $(109)_{10} = (6D)_{16}$.

But a quicker way is to use the binary notation: starting from the right, take the bits (*b*inary dig*its*) in groups of 4, and convert each group to base 16 using this table:

$0000 = 0$	$0001 = 1$	$0010 = 2$	$0011 = 3$
$0100 = 4$	$0101 = 5$	$0110 = 6$	$0111 = 7$
$1000 = 8$	$1001 = 9$	$1010 = \text{A}$	$1011 = \text{B}$
$1100 = \text{C}$	$1101 = \text{D}$	$1110 = \text{E}$	$1111 = \text{F}$

Thus $(109)_{10} = (0110\ 1101)_2 = (6D)_{16}$.

Now you try:

Convert $(10110101)_2$ to:
(a) decimal (base 10)
(b) octal (base 8)

(a) $(10110101)_2 = 2^7 + 2^5 + 2^4 + 2^2 + 2^0$
$= 128 + 32 + 16 + 4 + 1 = (181)_{10}$.

(b) $(10\ 110\ 101)_2 = (265)_8$. By taking groups of three bits.

4.5. Greatest Common Divisor

Definition 4.5.1 (Greatest Common Divisor)

Let a and b be integers, not both zero. The greatest common divisor of a and b, denoted $\gcd(a, b)$, is the integer d satisfying:

(i) $d \mid a$ and $d \mid b$.

(ii) $\forall c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$ then $c \leq d$.

The greatest common divisor is also called the highest common factor.

Examples: Find $\gcd(72, 63)$ and $\gcd(10^{20}, 6^{30})$.

- Using prime factorization: $72 = 2^3 \cdot 3^2$, and $63 = 3^2 \cdot 7$. The gcd is therefore $3^2 = 9$.
- Using prime factorization: $10^{20} = 2^{20} \cdot 5^{20}$, and $6^{30} = 2^{30} \cdot 3^{30}$. Thus, gcd is 2^{20}.

More examples:

For any $a \neq 0$, what is $\gcd(a, 0)$?

Answer: $\gcd(a, 0) = a$, because obviously a divides a and 0, and is the largest such divisor.

What is $\gcd(0, 0)$?

Any integer k divides 0. Since there is no largest integer, there is no largest common divisor.

The definition of gcd does not guarantee its existence. Hence,

Proposition 4.5.2 (Existence of gcd)

For any integers a, b, not both zero, their gcd exists and is unique.

Proof:

1. Let $D = \{$ all common divisors of $a, b\}$.
2. Clearly, $1 \in D$, and $D \subseteq \mathbb{Z}$.
3. By assumption, one of a, b is non-zero. Let it be a, since $\gcd(a, b) = \gcd(b, a)$ by its definition, so we can swap the numbers to make a the non-zero number.
4. Also, $|a|$ is an upper bound for D, since no common divisor of a, b can be larger than this.
5. Thus by Well Ordering 2, there exists a greatest element d in D.
6. By Proposition 4.3.4, d is unique. ■

4.5.1. Euclid's algorithm

In practice, computing the gcd by prime factorization is too slow, especially when the numbers are large. Luckily, an efficient algorithm was given by Euclid way back in the year 300BC.

The key idea to find $\gcd(a, b)$ is based on two facts:

(i) $\gcd(a, 0) = a$.

(ii) $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of a/b.

Line (i) was explained in the previous slide.

For Line (ii), note that since $a = bq + r$, then any common divisor c of a, b must divide r by Theorem 4.1.1 (r is a linear combination of a, b.) Also, any common divisor of b, r must divide a for the same reason.

So (a, b) and (b, r) have the same set of common divisors, and thus their gcd's must be equal.

Euclid's Algorithm for gcd

```
def gcd(I, CAN):
    # assumes I>0, CAN>=0
    # computes gcd using Euclid's algorithmm

    while CAN > 0:
        DOIT = I % CAN
        (I, CAN) = (CAN, DOIT)

    return I
```

Let's trace Euclid's algorithm to calculate $\gcd(330, 156)$.

$$
\begin{aligned}
 & & & & \gcd(330, 156) \\
330 &= 156 \times 2 + 18 & \leftarrow & & \gcd(156, 18) \\
156 &= 18 \times 8 + 12 & \leftarrow & & \gcd(18, 12) \\
18 &= 12 \times 1 + 6 & \leftarrow & & \gcd(12, 6) \\
12 &= 6 \times 2 + 0 & \leftarrow & & \gcd(6, 0)
\end{aligned}
$$

Thus $\gcd(330, 156) = 6$.

Theorem 4.5.3 (Bézout's Identity)

Let a, b be integers, not both zero, and let $d = gcd(a, b)$. Then there exist integers x, y such that:

$$ax + by = d.$$

The proof is cumbersome to write, so we give a sketch instead.

Proof sketch:

Trace the execution of Euclid's algorithm on a, b.
The last line gives the gcd d.
Now work backwards to express d in terms of linear combinations of the quotients and remainders of the previous lines, until you reach the top.

Using the example of $\gcd(330, 156)$, we work as follows:

$$\begin{aligned} 6 &= 18 - 12 \times 1 &&= 18 + 12 \times (-1) \\ &= 18 + (156 - 18 \times 8) \times (-1) &&= 156 \times (-1) + 18 \times 9 \\ &= 156 \times (-1) + (330 - 156 \times 2) \times 9 &&= 330 \times 9 + 156 \times (-19) \end{aligned}$$

Thus $6 = 330 \cdot 9 + 156 \cdot (-19)$.

The above procedure is called the Extended Euclidean Algorithm, for obvious reasons.

Non-uniqueness of Bézout's Identity

There are multiple solutions x, y to the equation $ax + by = d$.

Once a solution pair (x, y) is found, additional pairs may be generated by $(x + \frac{kb}{d}, y - \frac{ka}{d})$, where k is any integer.

Proof sketch: $a(x + \frac{kb}{d}) + b(y - \frac{ka}{d}) = ax + \frac{kab}{d} + by - \frac{kab}{d} = d$.

Aiken & Dueet: A Love Story

Dueet is in trouble. He has been secretly courting Aiken, a pretty farm girl, for the past six months, sneaking into the girl's farm house when her parents were out.

Unfortunately, today he got caught by the girl's no-nonsense father. Father gives Dueet a test: if he passes, he gets to marry the girl; otherwise, never ever step foot on the farm again.

The test is this: fill a large trough in the field with exactly 1 litre of river water. Only two cans are available to scoop water from the river: one is exactly 9 litres when full, the other 7.

Help Dueet pass the test to win Aiken.


9 litres


7 litres

Since the cans must be completely full or empty when transferring water, Dueet is dealing with multiples of 7 and 9 litres. In other words, Dueet needs to solve the equation:

$$9x + 7y = 1.$$

Note that $\gcd(9, 7) = 1$. Using Bézout's Identity, it is straightforward to get: $9(4) + 7(-5) = 1$.

Thus, Dueet needs to pour in four cans of water into the trough using the 9-litre can, and then scoop out five cans using the 7-litre can.

Definition 4.5.4 (Relatively Prime)

Integers a and b are relatively prime (or coprime) iff $\gcd(a, b) = 1$.

Examples:

- 9 and 7 are coprime (from Aiken & Dueet's puzzle).
- 10 and 100 are not coprime, since $\gcd(10, 100) = 10$.
- In fact, for any integer $a > 1$, a and ka are not coprime for any integer k (because their gcd is a).
- Obviously, any two distinct primes p, q are coprime.

We can now prove this theorem:

Theorem 4.2.3

If p is a prime and $x_1, x_2, \ldots, x_n$ are any integers such that: $p \mid x_1 x_2 \ldots x_n$, then $p \mid x_i$, for some i $(1 \leq i \leq n)$.

Proof:

(by Induction)

1. Let $P(n) = (\ (p \mid x_1 x_2 \ldots x_n) \longrightarrow (p \mid x_i \text{ for some } i \in [1, n])\ )$
2. (Consider the base case $n = 1$:)
3. Clearly, $P(1)$ is true.

   ...

proof cont'd

4. For any $k \in \mathbb{Z}^+$: (Inductive step:)
5. Assume $P(k)$ is true.
6. That is, $(p \mid x_1 x_2 \dots x_k) \longrightarrow (p \mid x_i \text{ for some } i \in [1, k])$.
7. (Consider the case $k + 1$:)
8. Suppose $p \mid x_1 x_2 \dots x_{k+1}$:
9. Let $A = x_1 x_2 \dots x_k$, so that $p \mid A x_{k+1}$.
10. If $p \mid A$:
11. Then $p \mid x_i$ for some $i \in [1, k]$ by the Inductive hypothesis. So $P(k + 1)$ is true.

...

proof cont'd

12. Else $p \nmid A$:
13. Then $\gcd(p, A) = 1$, because p is prime and $p \nmid A$.
14. Then there exist integers r, s such that $pr + As = 1$ by Bézout's Identity.
15. Now, $x_{k+1} = 1 \cdot x_{k+1} = (pr + As)x_{k+1}$
$= p(rx_{k+1}) + (Ax_{k+1})s$ by basic algebra.
16. Since p divides both terms, it divides their linear combination by Theorem 4.1.1.
17. Thus, $p \mid x_{k+1}$ and $P(k + 1)$ is true.
18. Hence, by Mathematical Induction, the theorem is true. ■

Proposition 4.5.5

For any integers a, b, not both zero, if c is a common divisor of a and b, then $c \mid gcd(a, b)$.

Proof:

1. Take any two integers a, b, not both zero.
2. Let $d = \gcd(a, b)$.
3. By Bézout's Identity, $d = ax + by$, for some integers x, y.
4. Suppose c is a common divisor of a, b:
5. Then $c \mid a$ and $c \mid b$, by definition of divisibility.
6. Thus $c \mid (ax + by)$ by Theorem 4.1.1
7. Thus $c \mid d$. ■

Example:
$\gcd(30, 45) = 15$.

$30 = 2 \cdot 3 \cdot 5$
$45 = 3^2 \cdot 5$.
Thus the common divisors are $1, 3, 5, 15$.

All of these common divisors divide 15.

Prove that for all positive integers a, b, $a \mid b$ if, and only if, $\gcd(a, b) = a$.

To prove "P iff Q", we need to prove "if P then Q" and "if Q then P".

Proof:

1. (Forward direction: "if P then Q")
2. For any positive integers a, b:
3. Suppose $a \mid b$:
4. Then $b = ak$ for some integer k, by definition of divisibility.
5. Then $\gcd(a, b) = \gcd(a, ak) = a$ because a is the largest common divisor.
6. (Backward direction: "if Q then P")
7. For any positive integers a, b:
8. Suppose $\gcd(a, b) = a$:
9. Then a is a common divisor of a, b, by definition of gcd.
10. Thus, $a \mid b$. ■

Now you try

Prove that if a, b are integers, not both zero, and $d = \gcd(a, b)$, then a/d and b/d are integers with no common divisor that is greater than 1.

4.6. Least Common Multiple

Definition 4.6.1 (Least Common Multiple)

For any non-zero integers a, b, their least common multiple, denoted $\text{lcm}(a, b)$, is the positive integer m such that:

(i) $a \mid m$ and $b \mid m$,

(ii) for all positive integers c, if $a \mid c$ and $b \mid c$, then $m \leq c$.

The lcm of a, b exists because the Well Ordering Principle guarantees the existence of the least element on the set of common multiples of a, b.

Examples: Find

- $\text{lcm}(12, 18)$
- $\text{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2)$
- $\text{lcm}(2800, 6125)$

- $12 = 2 \cdot 2 \cdot 3$, and $18 = 2 \cdot 3 \cdot 3$. The gcd is thus $2 \cdot 3 = 6$. The lcm is made up of the "factors other than the gcd", ie. lcm $= 2 \cdot 2 \cdot 3 \cdot 3 = 36$.
- The two numbers are: $2 \cdot 2 \cdot 3 \cdot 5$, and $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$. So the gcd $= 2 \cdot 2 \cdot 3 = 12$. And the lcm $= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 360$.
- $2800 = 2^4 \cdot 5^2 \cdot 7$, and $6125 = 5^3 \cdot 7^2$. Thus gcd $= 5^2 \cdot 7$, and lcm $= 2^4 \cdot 5^3 \cdot 7^2$.

From the above examples, it should be clear that

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$

Prove this as an exercise. Note that this provides an algorithm to compute the lcm. Write code to do this.

Now you try:

Prove that for all positive integers a and b, $\gcd(a, b) | \operatorname{lcm}(a, b)$.

Proof:

1. Take any non-zero integers a, b.
2. Let $d = \gcd(a, b)$, and $m = \operatorname{lcm}(a, b)$.
3. Then $d \mid a$ and $d \mid b$, by definition of gcd.
4. Also, $a \mid m$ and $b \mid m$, by definition of lcm.
5. Thus $d \mid m$, by the Transitivity of Divisibility (Theorem 4.3.3 (Epp)). ■

4. Number Theory (Part 3)

Terence Sim

Young man, in mathematics you don't understand things. You just get used to them.

If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is.

John von Neumann,
1903 — 1957

Reading

Sections 8.3 (from page 473), 8.4 of Epp.[1]

[1] Text in green are the corrections of errors.

4.7. Modulo Arithmetic

1 Sep. 2015 is a Tuesday. What day of the week is 30 Sep.?

Your friend messages you, saying, "I'll see you in three hours". Your phone shows 11:30am now. What time will your friend show up?

To answer both questions, you are doing modulo arithmetic.

Definition 4.7.1 (Congruence modulo)

Let m and n be integers, and let d be a positive integer. We say that m is congruent to n modulo d, and write:

$$m \equiv n \pmod{d}$$

if, and only if,

$$d \mid (m - n).$$

Symbolically: $m \equiv n \pmod{d} \Leftrightarrow d \mid (m - n)$

Examples: Determine which of the following is true and which is false.

- $12 \equiv 7 \pmod{5}$
- $6 \equiv -8 \pmod{4}$
- $3 \equiv 3 \pmod{7}$
- $\forall a, b \in \mathbb{Z}$, not both zero, $a \equiv b \pmod{\gcd(a, b)}$

Answer:

- True. Clearly, $5 \mid (12 - 7)$.
- False. Because $4 \nmid (6 - (-8))$.
- True. Since $7 \mid (3 - 3)$.
- True. Let $d = \gcd(a, b)$. Then $d \mid (a - b)$ because $d \mid a$ and $d \mid b$.

Theorem 8.4.1 (Epp): Modular Equivalences

Let a, b, and n be any integers and suppose $n > 1$. The following statements are all equivalent:

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ for some integer k
4. a and b have the same (non-negative) remainder when divided by n
5. $a \bmod n = b \bmod n$

Proof: see page 480 of Epp.

Note that $a \bmod n$ is the non-negative remainder r, when a is divided by n. By the Quotient-Remainder Theorem, $0 \leq r < n$. Another name for this is the residue of a modulo n.

4.7.1. Arithmetic

Theorem 8.4.3 (Epp): Modulo Arithmetic

Let a, b, c, d and n be integers with $n > 1$, and suppose:

$$a \equiv c \pmod{n} \text{ and } b \equiv d \pmod{n}.$$

Then

1. $(a + b) \equiv (c + d) \pmod{n}$
2. $(a - b) \equiv (c - d) \pmod{n}$
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$, for all positive integers m.

We will prove part 3. Try the rest yourself!

Proof:

1. For any integers a, b, c, d, n with $n > 1$:
2. Suppose $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$:
3. Then by Theorem 8.4.1 (Epp), there exist integers s, t such that $a = c + sn$ and $b = d + tn$.
4. Then $ab = (c + sn)(d + tn)$, by substitution.
5. $= cd + n(ct + sd + stn)$, by basic algebra.
6. Let $k = (ct + sd + stn)$. This is an integer by the closure property.
7. Thus $ab = cd + nk$.
8. By Theorem 8.4.1 (Epp), $ab \equiv cd \pmod{n}$. ■

A more useful form of part 3 is this Corollary:

Corollary 8.4.4 (Epp)

Let a, b, n be integers with $n > 1$. Then,

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n},$$

or, equivalently,

$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n.$$

In particular, if m is a positive integer, then

$$a^m \equiv [(a \bmod n)^m] \pmod{n}.$$

Example:

Calculate: (a) $55 \cdot 26 \bmod 4$, (b) $144^4 \bmod 713$

Answer:

$$\begin{aligned}(a)\quad 55 \cdot 26 \bmod 4 &= [(55 \bmod 4)(26 \bmod 4)] \bmod 4 \\ &= (3)(2) \bmod 4 \\ &= 6 \bmod 4 \\ &= 2\end{aligned}$$

$$\begin{aligned}(b)\quad 144^4 \bmod 713 &= (144^2)^2 \bmod 713 \\ &= (144^2 \bmod 713)^2 \bmod 713 \\ &= (20736 \bmod 713)^2 \bmod 713 \\ &= 59^2 \bmod 713 \\ &= 3481 \bmod 713 \\ &= 629\end{aligned}$$

4.7.2. Inverses

Normal arithmetic has the *Cancellation Law for Multiplication* (T7 of Appendix A (Epp)):

For integers a, b, c with $a \neq 0$, if

(1) $$ab = ac$$

then $b = c$.

This is not true in modulo arithmetic:

$$ab \equiv ac \pmod{n} \text{ does not imply } b \equiv c \pmod{n}$$

Example:

Clearly, $3 \times 1 \equiv 3 \times 5 \pmod{6}$.
But, $1 \not\equiv 5 \pmod{6}$.

When "cancelling" a on both sides of Equation (1), we are really multiplying with the multiplicative inverse of a. By definition, the multiplicative inverse is a number b such that $ab = 1$. Thus we need a suitable inverse that works with modulo arithmetic.

Definition 4.7.2 (Multiplicative inverse modulo n)

For any integers a, n with $n > 1$, if an integer s is such that $as \equiv 1 \pmod{n}$, then s is called the multiplicative inverse of a modulo n. We may write the inverse as a^{-1}.

Because the commutative law still applies in modulo arithmetic, we also have $a^{-1}a \equiv 1 \pmod{n}$.

Note that multiplicative inverses are not unique, since if s is such an inverse, then so is $(s + kn)$ for any integer k (Why?)

Example:

Consider $a = 5$ and $n = 9$: By inspection, $5 \cdot 2 \equiv 1 \pmod 9$, so $5^{-1} = 2 \bmod 9$.

Other multiplicative inverses include: $2+9 = 11$, $2-9 = -7$, $2 + 900 = 902$.

Given any integer a, its multiplicative inverse a^{-1} may not exist. This next theorem tells us exactly when it exists.

Theorem 4.7.3 (Existence of multiplicative inverse)

For any integer a, its multiplicative inverse modulo n (where $n > 1$), a^{-1}, exists if, and only if, a and n are coprime.

Recall that two numbers are coprime, or *relatively prime*, iff their gcd is 1.

Corollary 4.7.4 (Special case: n is prime)

If $n = p$ is a prime number, then all integers a in the range $0 < a < p$ have multiplicative inverses modulo p.

Proof: (Forward direction)

1. For any integers a, n with $n > 1$:
2. If a^{-1} exists:
3. Then $a^{-1}a \equiv 1 \pmod{n}$, by definition of multiplicative inverse.
4. Then $a^{-1}a = 1 + kn$, for some integer k, by Theorem 8.4.1 (Epp).
5. Re-write: $aa^{-1} - nk = 1$, by basic algebra.
6. (Claim: all common divisors of a and n are ± 1.)
7. Take any common divisor, d, of a and n.
8. $d \mid a$ and $d \mid n$ by definition of common divisor.
9. So $d \mid 1$ by Line 5 and Theorem 4.1.1.
10. Thus, $d = 1$ or $d = -1$ by Theorem 4.3.2 (Epp).
11. Hence $\gcd(a, n) = 1$.

Proof: (Backward direction)

1. For any integers a, n with $n > 1$:
2. If $\gcd(a, n) = 1$:
3. Then by Bézout's Identity, there exists integers s, t such that $as + nt = 1$.
4. Thus $as = 1 - tn$, by basic algebra.
5. Then by Theorem 8.4.1 (Epp), $as \equiv 1 \pmod{n}$. ■

Note that the above tells us how to find a multiplicative inverse for a modulo n: simply run the Extended Euclidean Algorithm!

Example:

Find 3^{-1} mod 40.

1. Since 3 is prime, and $40 = 2^3 \cdot 5$, it is easy to see that $\gcd(3, 40) = 1$.
2. Also, note that $40 = 3(13) + 1$.
3. Re-write: $3(-13) = 1 - 40$.
4. Thus by Theorem 8.4.1 (Epp), $3(-13) \equiv 1 \pmod{40}$.
5. Thus $3^{-1} = -13 \bmod 40$.

But this is ugly. We prefer a positive inverse. This can be corrected simply by adding a multiple of 40, eg. $-13 + 40 = 27$. Hence $3^{-1} = 27 \bmod 40$.

Example:

Find $2^{-1} \bmod 4$.

Note that $\gcd(2, 4) = 2$, so 2 and 4 are not coprime. Thus, by Theorem 4.7.3, 2^{-1} does not exist.

Indeed, we can check this:

$$\begin{aligned} 2 \cdot 1 &\equiv 2 \pmod 4, \\ 2 \cdot 2 &\equiv 0 \pmod 4, \\ 2 \cdot 3 &\equiv 2 \pmod 4. \end{aligned}$$

By Theorem 8.4.3 (Epp), these calculations suffice to conclude that 2^{-1} does not exist.

The use of multiplicative inverses leads us to a Cancellation Law for modulo arithmetic:

Theorem 8.4.9 (Epp)

For all integers a, b, c, n, with $n > 1$ and a and n are coprime, if $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

Proof sketch

Since a and n are coprime, Theorem 4.7.3 guarantees the existence of a multiplicative inverse a^{-1}.

Multiply both sides of $ab \equiv ac \pmod{n}$ with a^{-1} gives the desired answer.

Quiz: In T7 of Appendix A (Epp) (Cancellation Law for integers), it is explicitly stated that $a \neq 0$. Yet the above theorem doesn't seem to require this. Why not?

Example:

Solve the equation $5x + 13y = 75$ for integers x, y.

1. Re-write: $5x = 75 - 13y$.
2. Then $5x \equiv 75 \pmod{13}$, by Theorem 8.4.1 (Epp).
3. Re-write: $5x \equiv 5 \cdot 15 \pmod{13}$.
4. Note that 5 and 13 are coprime.
5. Thus, $x \equiv 15 \pmod{13}$, by Theorem 8.4.9 (Epp).
6. Thus, $x \equiv 2 \pmod{13}$, because $15 \bmod 13 = 2$.
7. So $x = 2$ is a solution.
8. Substituting back into the equation: $5(2) + 13y = 75$.
9. And thus $y = 5$.

Other solutions include: $(x, y) = (15, 0), (-11, 10), (28, -5)$.

4.8. Summary

1. We have learned many things in Number Theory:
   (a) Divisibility
   (b) Primes and prime factorization
   (c) Well ordering principle
   (d) Quotient-Remainder Theorem
   (e) Number bases
   (f) Greatest common divisor
   (g) Modulo arithmetic
2. Yet we have merely scratched the surface of a deep and fascinating field that has many applications.
3. Many Open Questions remain in Number Theory. Now and then someone will announce a breakthrough in one of these Questions. It is fun to follow their development, even if we don't fully understand their esoteric proofs.