Number Theory
Class Activity 5
Math-T101 Spring 2014

Name: Serife Sevis

Problem 1. *What is an even number? Give all the definitions you can think about. Show a general representation for an even number, both algebraically and by picture.*

Definition of an even number:

1) a number which occurs as we skip counting by twos.

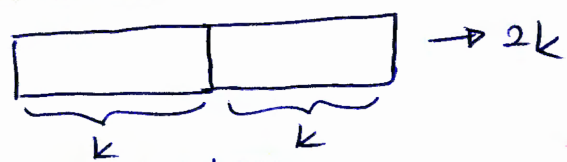
2) an even number of objects can be paired up (with none left unpaired)

3) a number which is twice a whole number

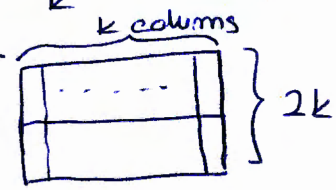
4) a number whose last digit is 0, 2, 4, 6, 8.

Algebraically: An even number is a number that can be written as $2k$ for some whole number k.

By picture:



OR



Problem 2. *What is an odd number? Give all the definitions you can think about. Show a general representation for an odd number, both algebraically and by picture.*

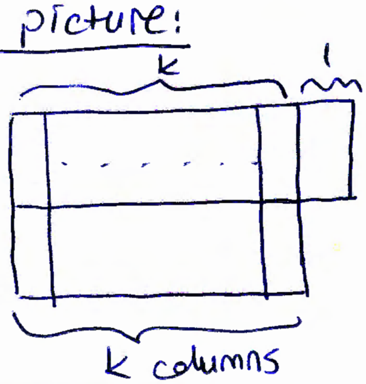
Defn. of an odd number:

1) a number which is 1 more than twice a whole number

2) a number whose last digit is 1, 3, 5, 7, 9.

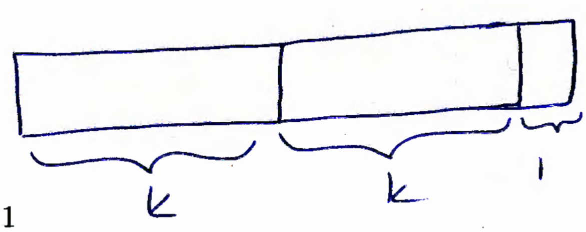
Algebraically: An odd number is a number that can be written as $2k+1$ for some whole number k
OR
written as $2k-1$ for some whole number $k \geq 1$

By picture:



$2k+1$

OR



$2k+1$

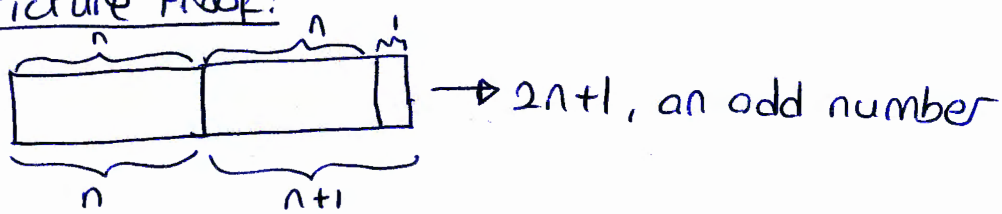
Problem 3. *Give a picture proof and an algebraic proof to show that the sum of two consecutive numbers is odd.*

Algebraic Proof:

Let n, $n+1$ be two consecutive numbers. Then,

$n + n+1 = 2n+1$, which is an odd number for wholenumbers n.

Picture Proof:



Problem 4. *Give a picture proof and an algebraic proof to show that sum of any three consecutive numbers is divisible by three.*

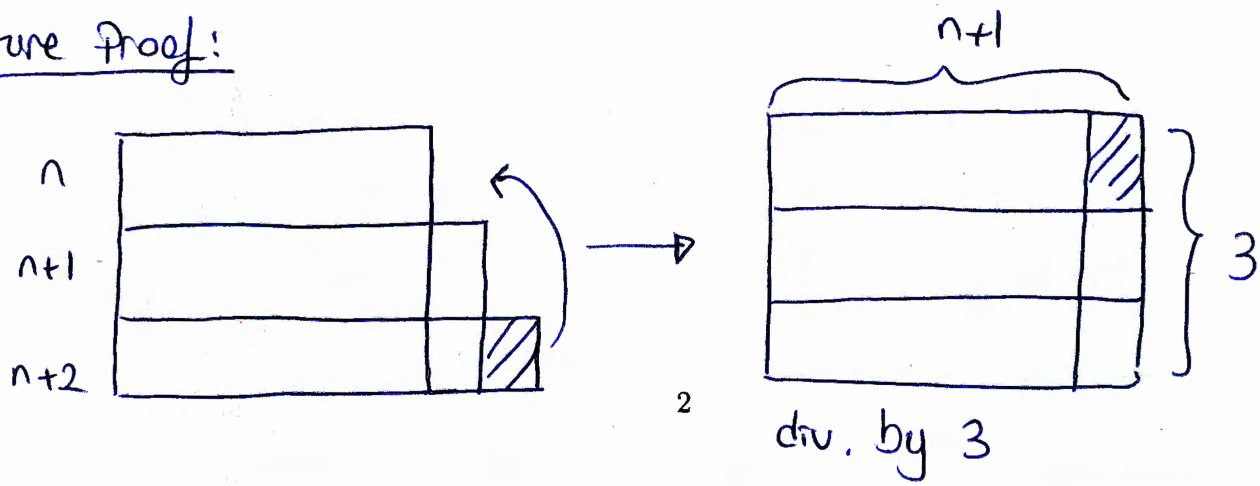
Algebraic Proof:

Let n, $n+1$, $n+2$ are three consecutive numbers

Then $n + n+1 + n+2 = 3n+3 = 3(n+1)$ by distributive property

which is a multiple of 3, and so the sum of three consecutive numbers is divisible by 3.

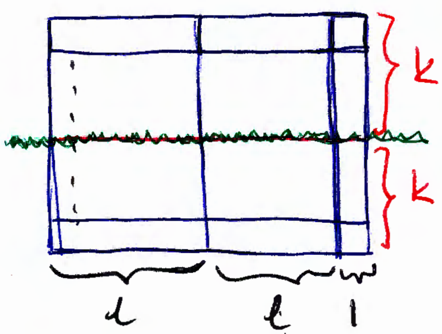
Picture Proof:



Problem 5. *Give a picture proof and an algebraic proof to show that the product of an even number and an odd number is even. For the picture proof use two different ways: First consider the horizontal dimension to be odd and vertical dimension to be even and then do it again vice versa.*

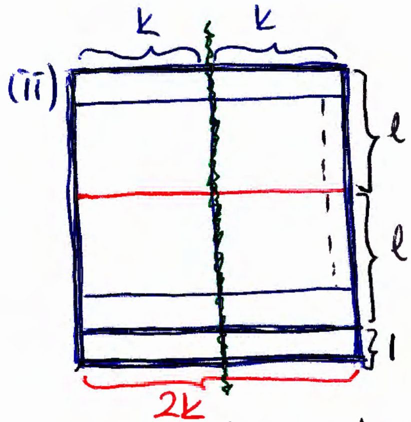
Picture Proof:

(i)



The number can be split into two equal groups, so the number is even (horizontally).

(ii)



The number can be split into two equal groups (vertically), so the number is even

Algebraic Proof:

Let A be an even number, so $A=2k$ for some whole number k. Let B an odd number, so $B=2l+1$ for some whole number l.

Then $A.B = (2k).(2l+1)$

$= 2k.(2l+1)$

$= 2k.2l + 2k$

(by dist. Prop.) $= 2(2kl+k)$

so $A.B$ is an even number.

Problem 6. *Give a picture proof and an algebraic proof to show the following: Suppose A is a number divisible by 7. Then B is divisible by 7 if and only if A + B is divisible by 7. (Please read pages 114-115 for the general case where 7 is replaced by k.)*

A is divisible by 7

B is divisible by 7 $\Longleftrightarrow$ A+B is divisible by 7

$\Rightarrow$ A is divisible by 7, so $A=7a$ for some whole number a.

if B is divisible by 7 then $B=7b$ for some whole number b.

Then $A+B = 7a+7b = 7(a+b)$ (by distributive property)

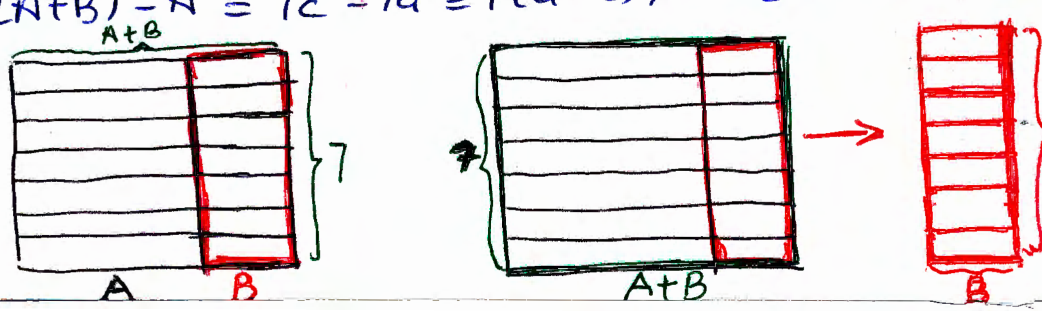
So A+B is divisible by 7.

$\Leftarrow$ A is divisible by 7, so $A=7a$ for some whole number a.

If A+B is divisible by 7, then $A+B=7c$ for some whole number c.

Then $B = (A+B) - A = 7c - 7a = 7(a-c)$, so B is divisible by 7.

Picture Proof:



Definition 1. *For any two whole numbers a and b,*

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

means that a and b have the same remainder when divided by k. Hence, $a \equiv 0 \pmod{k}$ *means that k is divisible by a.*

Example 1. *For example:* $3 \equiv 8 \pmod{5}$ *or* $8 \equiv 13 \pmod{5}$*. Give two more examples of congruence mod 5.*

$$1 \equiv 6 \pmod{5}$$

$$-1 \equiv 4 \equiv 9 \pmod{5}$$

Definition 2. *For any two* **integers** *a and b,*

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

if and only if $|a - b| \equiv 0 \pmod{k}$.

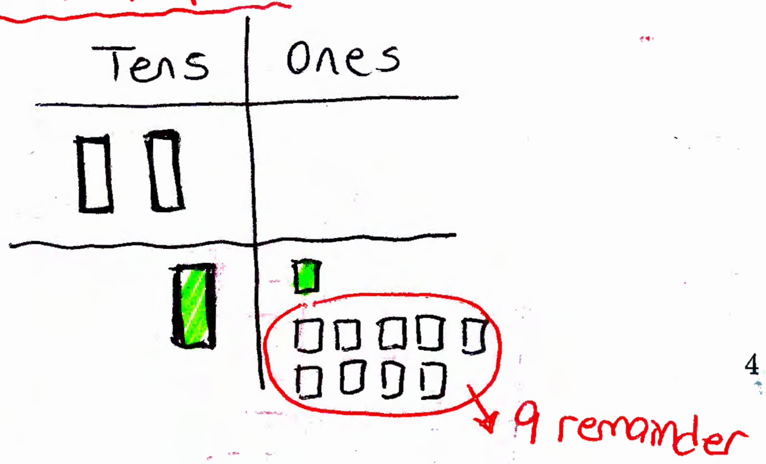
Example 2. *For example:* $-3 \equiv 8 \pmod{11}$*. Give two more examples of a negative and a positive number that are congruent mod 11.*

$$-6 \equiv 5 \pmod{11}$$

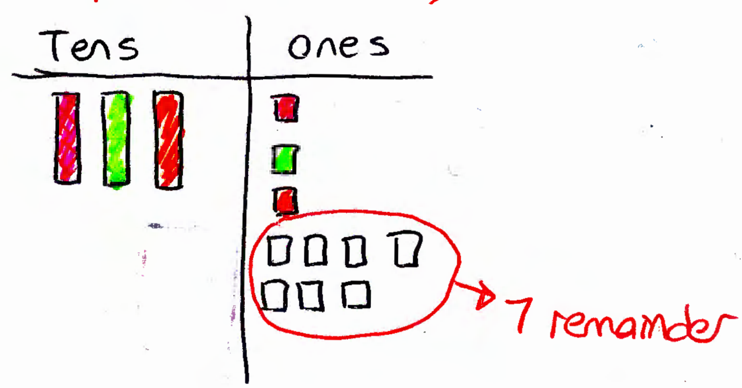
$$-6 \equiv 5 \equiv 16 \pmod{11}$$

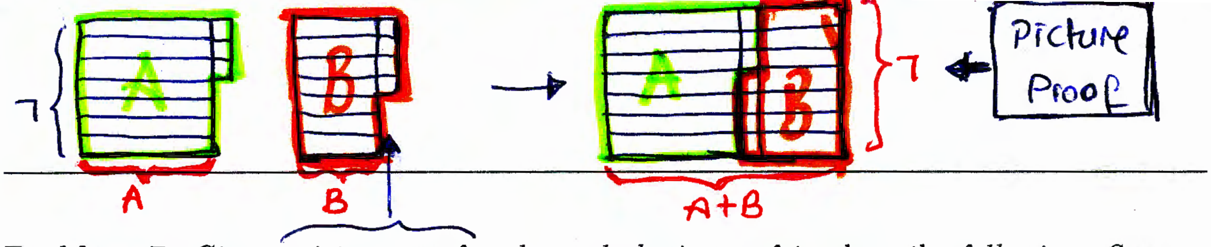
$$-2 \equiv \underbrace{9 \equiv 20} \pmod{11}$$

Other Examples



$$40 \equiv 7 \pmod{11}$$





Problem 7. *Give a picture proof and an algebraic proof to show the following: Suppose* $A \equiv 3 \pmod 7$ *and* $B \equiv 4 \pmod 7$. *Show that* $A + B \equiv 0 \pmod 7$.

Algebraic Proof:

$A \equiv 3 \pmod 7$ means $|A-3| \equiv 0 \pmod 7$

OR $A \equiv 3 \pmod 7$ means $A = 7k+3$ for some k

which means $A-3$ is divisible by 7. So, $A-3 = 7k$ for some whole number k.

$B \equiv 4 \pmod 7$ means $|B-4| \equiv 0 \pmod 7$.

which means $B-4$ is divisible by 7. So $B-4 = 7\ell$ for some whole number ℓ.

Then $A+B = (7k+3) + (7\ell+4) = 7k + 7\ell + 7 = 7(k+\ell+1)$

which means $A+B$ is divisible by 7. Thus $A+B \equiv 0 \pmod 7$

Problem 8. *Suppose* $A \equiv 6 \pmod 7$ *and* $B \equiv 5 \pmod 7$. *Fill in the blank with a whole number between 1 and 7:* $A + B \equiv$ 4 $\pmod 7$ *and prove your answer algebraically.*

If $A \equiv 6 \pmod 7$, then $A = 7k+6$ for some whole number k.

& If $B = 5 \pmod 7$, then $B = 7\ell+5$ for some whole number ℓ.

$$\begin{aligned} \text{Then } A+B &= 7k+6+7\ell+5 \\ &= 7k+7\ell+11 \\ &= 7k+7\ell+7+4 \\ &= 7(k+\ell+1)+4 \end{aligned}$$

which means $A+B \equiv 4 \pmod 7$

Problem 9. *Let N be a five-digit number, with digits abcde (note that a, b, c, d, and e are all one-digit numbers). (Actually, the result of this problem works for any number of digits, but for ease of notation we stick to 5 digits.) In expanded form* $N = 10000a + 1000b + 100c + 10d + e$.

a) Show that $N \equiv e \pmod{10}$.

if N=abcde, then $N = 10000a + 1000b + 100c + 10d + e$

$N = 10(1000a + 100b + 10c + d) + e$

which means $N \equiv e \pmod{10}$

b) Show that $N \equiv e \pmod{5}$.

If N=abcde, then $N = 10000a + 1000b + 100c + 10d + e$

$N = 5(2000a + 200b + 20c + 2d) + e$

which means $N \equiv e \pmod{5}$

c) Show that $N \equiv 0 \pmod{2}$ *if e is even.*

If N=abcde, then $N = 10000a + 1000b + 100c + 10d + e$

$N = 2(5000a + 500b + 50c + 5d) + e$

$N \equiv e \equiv 0$ if e is even ($e = 2k$ for some k.)

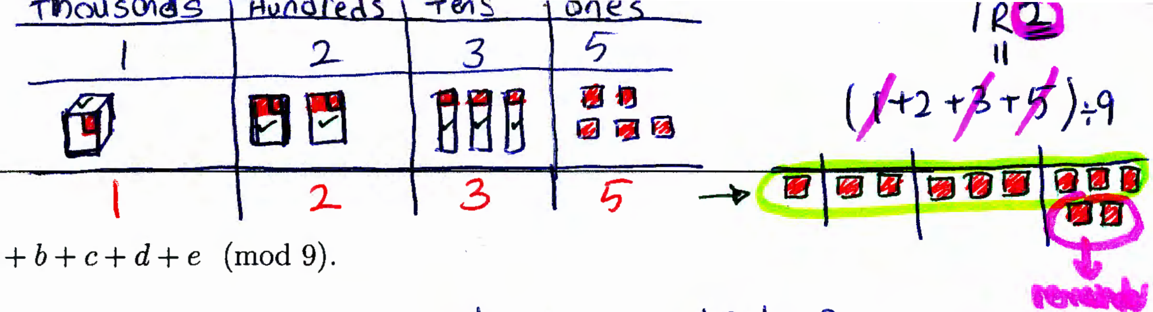
d) Show that $N \equiv 10d + e \pmod{4}$. *(Recall that d and e are the last two digits of N.)*

If N=abcde, then $N = 10000a + 1000b + 100c + 10d + e$

$N = 4(2500a + 250b + 25c) + 10d + e$

$N \equiv 10d + e \pmod{4}$

Picture proof



$1 R \, 2$

$(\cancel{1}+2+\cancel{3}+\cancel{5}) \div 9$

e) *Show that* $N \equiv a+b+c+d+e \pmod 9$.

If $N = abcde$, then $N = 10000a + 1000b + 100c + 10d + e$

$N = 9999a + 999b + 99c + 9d + (a+b+c+d+e)$

$N = 9(1111a + 111b + 11c + d) + (a+b+c+d+e)$

then $N \equiv a+b+c+d+e \pmod 9$

f) *Show that* $N \equiv a+b+c+d+e \pmod 3$.

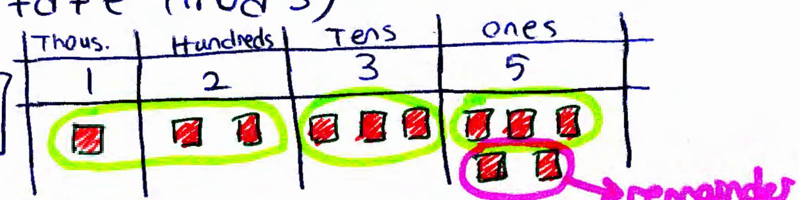
If $N = abcde$, then $N = 10000a + 1000b + 100c + 10d + e$

$= 9(1111a + 111b + 11c + d) + (a+b+c+d+e)$

$= 3(3333a + 333b + 33c + 3d) + (a+b+c+d+e)$

then $N \equiv a+b+c+d+e \pmod 3$

[See the picture proof above]



$(\cancel{1}+2+\cancel{3}+\cancel{5}) \div 3 = 3 \; R \, 2$

g) *Show that* $N \equiv (a+c+e) - (b+d) \pmod{11}$.

If $N = abcde$, then $N = 10000a + 1000b + 100c + 10d + e$

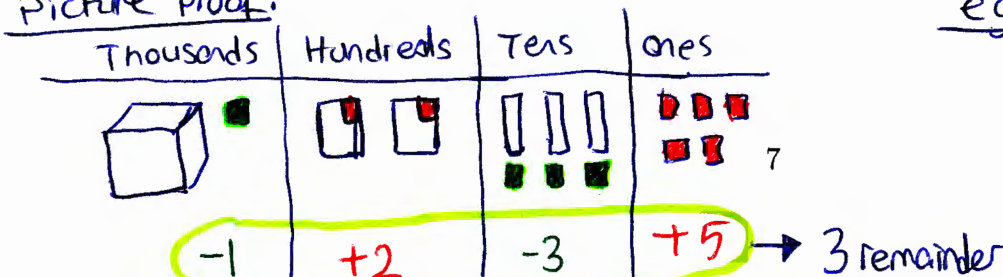
$N = 9999a + a + 1001b - b + 99c + c + 11d - d + e$

$N = [9999a + 1001b + 99c + 11d] + (a - b + c - d + e)$

$N = 11[909a + 91b + 9c + d] + [(a+c+e) - (b+d)]$

Then $N \equiv (a+c+e) - (b+d) \pmod{11}$

Picture Proof:



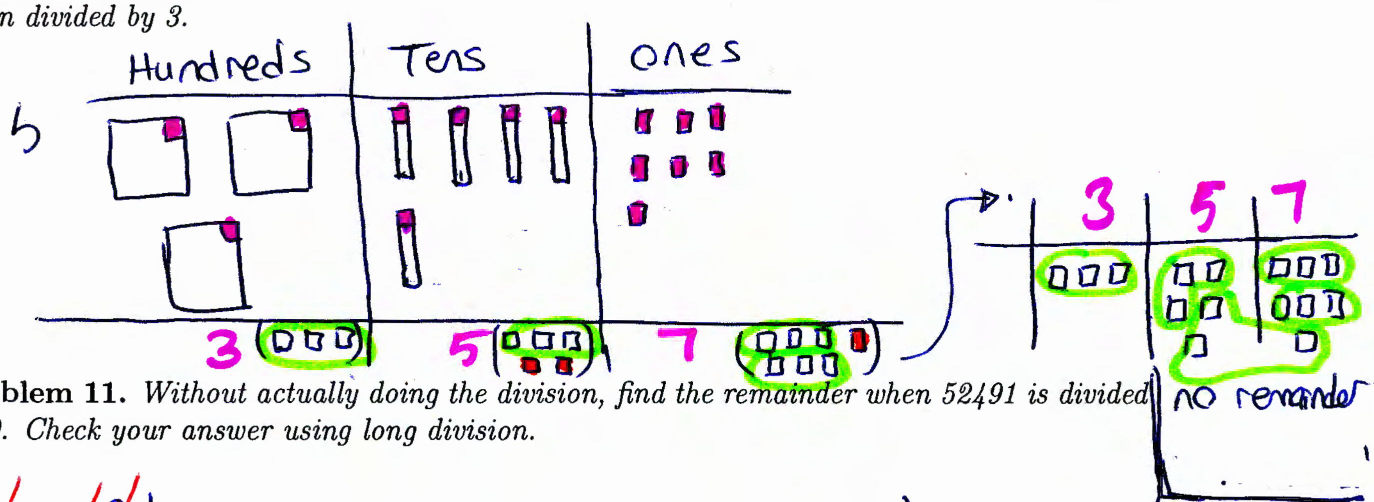
eg: 1235

$- + - +$

$-1 + 2 - 3 + 5 = 3$

$1235 \equiv 3 \pmod{11}$

Problem 10. *Using base blocks (without using long division) show the remainder of 357 when divided by 3.*



Problem 11. *Without actually doing the division, find the remainder when 52491 is divided by 9. Check your answer using long division.*

$\cancel{5}2\cancel{4}\cancel{9}1$

$2+1=3$

$$52491 \equiv 3 \pmod 9$$

The idea behind casting out

$(5+2+4+9+1) \div 9 \Rightarrow$ among this number eliminate *s divisible by

Problem 12. *Another example of mod 11 arithmetic: Find the remainder of 7493 divided by 11 without using long division.*

$$\underset{-\,+\,-\,+}{7493} \rightsquigarrow -7+4-9+3 = (4+3)-(7+9)$$
$$= -9$$

$$7493 \equiv -9 \equiv 2 \pmod{11}$$

Problem 13. *Add the three numbers below, and check your answer by casting out 9's.*

$$\begin{array}{r} \cancel{7}\cancel{5}8\cancel{2} \\ \cancel{6}\cancel{2}\cancel{4}\cancel{8} \\ +\ \cancel{3}\cancel{1}\cancel{9}\cancel{7} \\ \hline 17027 \end{array}$$

$$17027 \equiv 8 \pmod 9$$

Definition 3. *A prime number is a whole number $P > 1$ whose only factors are 1 and P. Whole numbers $N > 1$ which are not prime are called composite.*

Note: Based on this definition, 0 and 1 are neither prime nor composite.

Problem 14. Sieve of Eratosthenes. *In the array below, cross off all numbers that are not prime.*

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~
~~49~~	~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71	~~72~~
73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~
~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~
97	~~98~~	~~99~~	~~100~~	101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~

Lemma: Prove that every whole number $N > 1$ is divisible by a prime.

Given N, list of all of its factors and let p be the smallest factor which $p>1$.
Then N is a multiple of P, say $N = pq$. This means that N is divisible by p. $[1<p<N]$
Suppose that p is not prime, then p has factors as $r.s = p$. Then r & s are factors of N since $N = p.q = r.s.q$ and $r \leq p$ & $s < p$. But no factor of N is smaller than p, except 1. Thus, r is either 1 or p. So p is a prime and N is divisible by a prime ∎

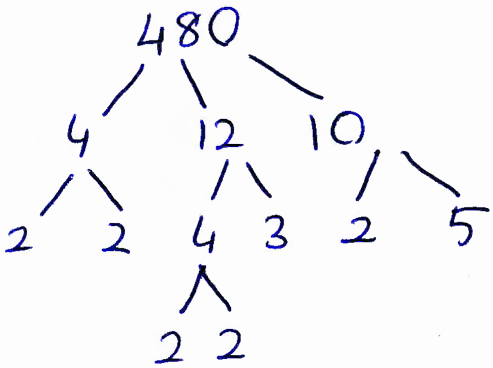
Fundamental Theorem of Arithmetic (Part 1): Every whole number $N > 1$ can be written as a product of primes.

Proof:

From Lemma (above), N can be written as $N = p_1 . n_1$ for some prime p_1.
If $n_1 = 1$ and then $N = p_1$ is prime. Then we are done.
If $n_1 \neq 1$ then n_1 can be written as $n_1 = p_2 . n_2$ for a prime p_2.
So $N = p_1 . p_2 . n_2$
Again if $n_2 = 1$ then $N = p_1 . p_2$ and we are done. If not, we can repeat and write as $N = p_1 . p_2 . p_3 . p_4 \cdots p_k . n_k$ where $n_k = 1$. Then $N = p_1 . p_2 . p_3 . \cdots p_k$ is written as the product of primes ∎

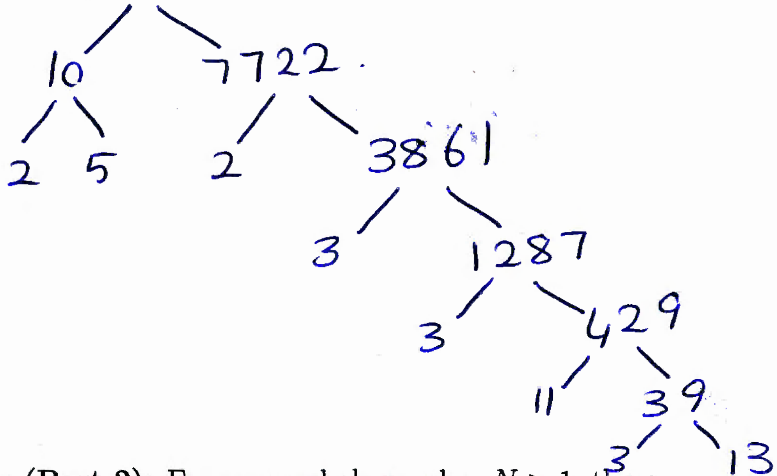
Problem 15. *Find the prime factorization of each of the following numbers and write it in exponential form.*

a) 480



$480 = 2^5 \cdot 3 \cdot 5$

b) 77220 $= 2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 13$



Fundamental Theorem of Arithmetic (Part 2): For every whole number $N > 1$, there is only one way of writing N as a product of primes, except for reordering.
Part 2 will be proved later, in Section 5.5, but you are allowed to use it in your current work.

Example 1. It is easy to see that $7 \cdot 19 \cdot 23^2 = 23 \cdot 7 \cdot 19 \cdot 23$, because this is just a reordering of the factors. This does not violate the Fundamental Theorem, because reordering is allowed.

Example 2: Without doing the multiplication, we can show that $19 \cdot 23^2 \cdot 7 \neq 13^2 \cdot 29 \cdot 17$. Explain why this follows from Part 2 of the Fundamental Theorem of Arithmetic.

$\underbrace{19 \cdot 23^2 \cdot 7}_{\text{this number has prime factors } 19,23,7} \neq \underbrace{13^2 \cdot 29 \cdot 17}_{\text{this number has prime factors } 13,29,17}$

Those are two different numbers because each number has a unique way of being written as product of primes.

Example 3: Without doing any multiplication or division, how can we show that $11^2 \cdot 29^5$ is not divisible by 21?

If N is divisible by 21, then it has to be divisible by 3 & 7 (i.e $21 = 3 \cdot 7$) since 7 & 3 are not factors of $11^2 \cdot 29^5$, so it is not divisible by 21.

Example 4: We can write $21 = 3 \cdot 7$ and $21 = 1 \cdot 3 \cdot 7$. Explain why this does not violate Part 2 of the Fundamental Theorem of Arithmetic.

Because 1 is not a prime number, $21 = \underbrace{3 \cdot 7}_{} = \underbrace{1 \cdot 3 \cdot 7}_{}$ has a unique prime factorization.
both are the same prime factorization

Definition 4. *The number* $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot \ldots \cdot n$ *is written as* $n!$ *and called "n factorial".*

Example 5: $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6!$

Problem 16. *Write the prime factorization of* 12! *in exponential form.*

$12! = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

$2^2 \quad 3 \qquad 2 \quad 5 \quad 3^2 \quad 2^3 \quad 2 \cdot 3 \quad 2^2$

$12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$

Problem 17. *Is* 12! *divisible by 7? By 40? By 120? By 1000?*

$12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$

$7 = 7 \cdot 1$; since 7 is one of the factors of 12!, 12! is divisible by 7.

$40 = 2^3 \cdot 5$; since 2^3 and 5 are the factors of 12!, it is div. by 40

$120 = 12 \cdot 10 = 2^3 \cdot 3 \cdot 5$; since 2^3, 3, and 5 are facters of 12!, it is divisible by 120. [it should have this many prime factorization]

$1000 = 10^3 = 2^3 \cdot 5^3$; 2^3 is a factor of 12!, but 5^3 is not a factor of 12!.
So, it is not divisible by 1000.

12! includes 5^2, but not 5^3

Problem 18. *How many zeros are at the end of the decimal form of* 30!?

$$30! \to \underbrace{\begin{matrix} 5, & 10, & 15, & 20, & 25, & 30 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5^1 & 5^1 & 5^1 & 5^1 & 5^2 & 5^1 \end{matrix}}_{5^7}$$

So, 30! has 7 zeros at the end.

(*) # of zeros at the end of the number = # of 10s in this number

$10 = 2.5$

so we are looking for # of 5s and # of 2s. Since half of the numbers in 30! even, there are at least 15 even numbers, so there are at least 2^{15}. That's why it is enough to look for the number of 5s.

Problem 19. *Is* 25! *divisible by 143,000,000?*

$$143{,}000{,}000 = 143 \cdot 10^6$$
$$= 11 \checkmark \cdot 13 \checkmark \cdot 10^6 \checkmark$$
$$= 2^6 \cdot 5^6 \cdot 11 \cdot 13$$

$25! = 25 \cdot 24 \cdot 23 \cdot \ldots \cdot 2 \cdot 1$

$$25! \to \underbrace{\begin{matrix} 5, & 10, & 15, & 20, & 25 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5^1 & 5^1 & 5^1 & 5^1 & 5^2 \end{matrix}}_{5^6}$$

There are 6 zeros at the end of 25!. So there are 6 tens (10^6)

25! is divisible by 143,000,000 because 25! has all the factors of 143,000,000.

Fact 1. *A whole number $N > 1$ is prime unless it has a prime factor $p \le \sqrt{N}$. Thus to test whether N is prime or not, one only needs to check divisibility by the primes $p = 2, 3, 5, \ldots$ satisfying $p^2 \le N$.*

Note: If N is composite, it can be written as pn, where p is the smallest factor of N (other than 1). Then p must be prime, and $p^2 \le np = N$. Therefore $p \le \sqrt{N}$.

Problem 20. *Show that 247 is not divisible by 2,3,5,7,11, applying the divisibility tests whenever possible. Is 247 prime? If so, explain why. If not, write 247 as a product of primes.*

$13^2 = 169 < 247 \longrightarrow$ check $13, 11, 7, 5, 3, 2$
✓ ✗ ✗ ✗ ✗ ✗

$17^2 = 289 > 247$

$247 = 13.19$ so it is not prime

Problem 21. *Find the prime factorization of each of the following numbers and write it in exponential form.*

a) $1771 = 11.161$
$= 11.7.23$
$= 7.11.23$

b) $2261 = 7.323$
$= 7.17.19$

Problem 22. *Show that* $11!+2$, $11!+3$, $11!+4$, $\ldots$, $11!+11$ *are all composite by giving a factor of each.*

$11!+2 = \underline{2}.(3.4.5.6.7.8.9.10.11+1) \rightarrow 11!+2$ is div. by 2

$11!+3 = \underline{3}.(2.4.5.6.7.8.9.10.11+1) \rightarrow 11!+3$ is div. by 3

$11!+4 = \underline{4}.(2.3.5.6.7.8.9.10.11+1) \rightarrow 11!+4$ is div. by 4

$\vdots$

$11!+11 = \underline{11}.(2.3.4.5.6.7.8.9.10+1) \rightarrow 11!+11$ is div. by 11

$11!+2, 11!+3, 11!+4, \ldots, 11!+11$ are composites because they can be written as product of smaller ~~#~~s.

(11!+12 is composite because 12 = 2.6 = 3.4 has factors in 11!, But 11!+13 is prime)

Problem 23. *Can you find any factors of* 11! + 1*? Do any of the primes 2,3,5,7,11 divide* 11! + 1*?*

$11!+1 = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11+1$ → not divisible by those primes.

$= 1\cdot \underbrace{(2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11+1)}_{11!+1}$

The factors are 1 and itself (11!+1)

So, 11!+1 is prime.

But still we need to check largest square of the prime. (fact 1)

Problem 24. *Can you find a list of 7 consecutive composite numbers? How about 70?*

$\left.\begin{array}{l} 8!+2 \\ 8!+3 \\ 8!+4 \\ 8!+5 \\ 8!+6 \\ 8!+7 \\ 8!+8 \end{array}\right\}$ 7 consecutive composite numbers

17 consecutive numbers

18!+2

18!+3

18!+4

⋮

18!+18

OR start 19!, 20!, start with a number bigger than 17.

70 consecutive numbers: 71!+2, 71!+3, 71!+4, ... 71!+71

Theorem: Given any positive whole number n that you like, we can make a list of n consecutive numbers, where all of these numbers are composite.

Proof:

Let n be a whole number $(n \geq 1)$. Then $(n+1)!+2$ is divisible by 2 because both $(n+1)!$ and 2 are divisible by 2.

Then $(n+1)!+3$ is divisible by 3

$(n+1)!+4$ is divisible by 4

⋮

$(n+1)!+n$ is divisible by n

$(n+1)!+n+1$ is divisible by $n+1$

So, the list of numbers $(n+1)!+2, (n+1)!+3, \dots, (n+1)!+n+1$ is the list of n consecutive numbers where all of them are composite.

Theorem: There are infinitely many primes.

Proof: Suppose that there are only finitely many primes, let's say n of them. We denote them by $p_1, p_2, p_3, \ldots, p_n$. Now construct a new number $p = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$. Clearly, p is larger than any of the primes, so, it does not equal to one of them. Since $p_1, p_2, p_3, \ldots, p_n$ constitute all primes, p cannot be prime. Thus, it must be divisible by at least one of our finitely many primes, say p_n.

But when we divide p by p_n, we get a remainder 1. Thus p is not a multiple of any prime. But that contradicts the fact that every whole number is a multiple of primes. This contradiction means that our assumption that there are finitely many primes is not correct. There are infinitely many primes.

Problem 25. *Is $n! + 1$ prime for every whole number n?*

NO!

Counter example: $5! + 1 = 1.2.3.4.5 + 1 = 120 + 1$

$5! + 1 = 121$ is a composite number

$4! + 1 = 24 + 1 = 25$ is composite number not prime.

Problem 26. *Find GCF(24, 88) in two different ways: by listing the factors and by finding the prime factorization.*

$24 = \underline{2^3} \cdot 3$

$88 = \underline{2^3} \cdot 11$

$GCF(24, 88) = 2^3 = 8$

Problem 27. *Find GCF(990, 825) in two different ways: by finding the prime factorization and by using the Euclidean algorithm.*

$$825 \overline{)990} = 1,\quad 990 - 825 = 165$$

$$165 \overline{)825} = 5,\quad 825 - 825 = 0$$

GCF (990, 825) = 165

Euclidean Algorithm

Prime factorization

$990 = 2 \cdot 3^2 \cdot 5 \cdot 11$

$825 = 3 \cdot 5^2 \cdot 11$

GCF (990, 825) = $3 \cdot 5 \cdot 11$
= 165

Problem 28. *Use the Euclidean algorithm to find GCF(1081, 1457).*

$$1081 \overline{)1457} = 1,\quad 1457 - 1081 = 376$$

$$376 \overline{)1081} = 2,\quad 1081 - 752 = 329$$

$$329 \overline{)376} = 1,\quad 376 - 329 = 47$$

$$47 \overline{)329} = 7,\quad 329 - 329 = 0$$

GCF (1081, 1457) = 47

Problem 29. *a) Use the Euclidean algorithm to find GCF(133,943).*

$$133\overline{)943}\quad 7,\quad -931,\quad 12$$

$$12\overline{)133}\quad 11,\quad -12,\quad 13,\quad -12,\quad 1$$

$$1\overline{)12}\quad 12,\quad -1,\quad 2,\quad -2,\quad 0$$

GCF (133, 943) = 1

$\boxed{943 = 133.7 + 12}$ ①

$\boxed{133 = 12.11 + 1}$ ②

$12 = 1.12 + 0$

b) (Extended Euclidean Algorithm) Find integers m and n such that $943n + 133m = 1$.

② $\boxed{1 = 133 - 12.11}$ $\longrightarrow$

① $\boxed{12 = 943 - 133.7}$

$$1 = 133 - 12.11$$
$$= 133 - (943 - 133.7).11$$
$$= 133 - (943.11 - 133.77)$$
$$= 133 - 943.11 + 133.77$$
$$= 133.(78) - 943.(11)$$
$$= 943.(-11) + 133.(78)$$

$m = 78$

$n = -11$

Lemma 1 (used in Euclidean Algorithm): If $a = bq + r$ then $GCF(a, b) = GCF(b, r)$.

If n is a factor of both b and r, then it is also a factor of $a = bq + r$ because $bq + r$ is a multiple of n.
Similarly, if n is a factor of both a & b then it is also a factor of $r = a - bq$. So the sets of

$\{CF(a,b)\}$ & $\{CF(b,r)\}$ are identical. Thus, the largest number in the first list = $GCF(a,b)$ is the same as the largest number in the second list = $GCF(b,r)$.

Definition 5. *Two whole numbers a and b are called relatively prime if $GCF(a, b) = 1$.*

Lemma 2: For any whole numbers a and b, that are relatively prime, there are integers m and n where $ma + nb = 1$. → linear combination

We can look back at the Extended Euclidean Algorithm to check this Lemma.

Problem 30. *For example, find integers m and n so that $1265m + 241n = 1$.*

$$\begin{array}{r} 5 \\ 241\overline{)1265} \\ -1205 \\ \hline 60 \end{array} \quad \rightarrow \quad \begin{array}{r} 4 \\ 60\overline{)241} \\ -240 \\ \hline 1 \end{array} \quad \rightarrow \quad \begin{array}{r} 60 \\ 1\overline{)60} \\ -6 \\ \hline 00 \end{array}$$

$1265 = 241 \cdot 5 + 60$

$\boxed{60 = 1265 - 241 \cdot 5}$

$\boxed{241 = 60 \cdot 4 + 1}$

$1 = 241 - 60 \cdot 4$

$1 = 241 - (1265 - 241 \cdot 5) \cdot 4$

$1 = 241 - (1265 \cdot 4 - 241 \cdot 20)$

$1 = 241 - 1265 \cdot 4 + 241 \cdot 20$

$1 = 241 \cdot 21 - 1265 \cdot 4$

$1 = 1265 \cdot (-4) + 241 \cdot (21) \rightarrow m = -4,\ n = 21$

Lemma 3: If p is a prime number and p is not a factor of a, then p and a are relatively prime.

Given: p is prime and p is not a factor of a

Prove: $GCF(p,a)=1$

If p is a prime & p is not a factor of a, then $GCF(p,a)$ is either 1 or p because p has only factors 1 and p. If $GCF(p,a)$ is 1, then you're done.
If $GCF(p,a)=p$. Then p is a factor of a. Contradiction! $GCF(p,a)$ is not p because p is not a factor of a.

Lemma 4: If p is a prime factor of ab, then p is a factor of either a or b.

Given: p is a factor of ab

Prove: p is a factor of a or p is a factor of b.

If p is a factor of a, then we're done.
Let's assume p is not a factor of a, then p and a are relatively prime
so, $GCF(p,a)=1$

Therefore, there are two integers m, n such that
$mp+na=1$
$b(mp+na=1)$
$bmp+bna=b$
$bmp+nab=b$
since we know p is a factor of ab, then $ab=p.k$
$bmp+npk=b \rightarrow p.(bm+nk)=b \rightarrow$ so p is a factor of b

Fundamental Theorem of Arithmetic (Part 2): For every whole number $N > 1$, there is only one way of writing N as a product of primes, except for reordering.

Here we use an example to display the reasoning for the proof of part 2 of the Fundamental Theorem of Arithmetic. Let's look at $51425 = 5^2 \cdot 11^2 \cdot 17$. Assume that this number has another prime factorizations $p_1 \cdot p_2 \ldots p_n$.

FTA (part 2): $51425 = \underbrace{5}_{a} \cdot \underbrace{(5 \cdot 11^2 \cdot 17)}_{b}$

P_1 is a factor of ab, then P_1 is a factor of either 5 or $5.11^2.17$ by lemma 3.

Then it is 5 $(P_1=5)$

keeps going for each prime.

Problem 31. *Find LCM(24, 88) using the prime factorizations.*

$24 = 2^3 \cdot 3$

$88 = 2^3 \cdot 11$

$$\mathrm{LCM}(24, 88) = \overbrace{\underbrace{2^3 \cdot 3}_{24} \cdot 11}^{88}$$

lowest common multiple

Good checking method: Both 24 and 88 will go in it, so
LCM > 24
& LCM > 88.

Problem 32. *Find LCM(10, 24, 88) using the prime factorizations.*

$10 = 2 \cdot 5$

$24 = 2^3 \cdot 3$

$88 = 2^3 \cdot 11$

$\mathrm{LCM}(10, 24, 88) = 2^3 \cdot 3 \cdot 5 \cdot 11$

Problem 33. Find $\mathrm{LCM}(a, b) = ?$

if $a = 2^2 \cdot 3^2 \cdot 5^3$

$b = 3^3 \cdot 5 \cdot 7$

$\mathrm{LCM}(a, b) = 2^2 \cdot 3^3 \cdot 5^3 \cdot 7$