ICPS - Oct 11 and Oct 18

1 A Rough introduction to Number Theory and Diophantine Equations

1.1 Number Theory

We will start with numbers and then to the theory. We have many sets of numbers, we will be concerned with only these two

$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$ the natural numbers, and
$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, \ldots\}$ the integers.

We know how to do many things with these numbers: add, subtract, multiply and divide. However, when we divide we may write it differently here:

$$\begin{array}{r} 7 \quad \text{R } 2 \\ 3\,\overline{)23} \end{array}$$

will be written as $23 = 3 \cdot 7 + 2$. In general that is a divided by b is written as

$$a = b \cdot q + r$$

where q is called the **quotient** and r is the **remainder**. And $0 \leq r < b$. Important point here is that the q and r are unique. This fact is important and not true for all sets of numbers. But it is true for $/Z$.

Definition 1.1. *We say a* **divides** *b (written $a|b$) if when we divide a by b we get a remainder of zero. Equivalently we can say $a|b$ if and only if there is some $k \in \mathbb{Z}$ so that$b = ka$. We call b a* **divisor** *of a.*

Definition 1.2. *We say $p \in \mathbb{N}$ is a* **prime** *if the only divisors of p are 1 and itself.*

Theorem 1.3 (Euclid)**.** *There are infinitely many primes.*

Proof. Assume there are are only finitely many primes (toward a contradiction). Let's list all primes: $p_1, p_2, p_3, \ldots, p_n$.

Define $x = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n + 1$.

Note dividing x by p_i yields $x = p_i q + 1$. So $p_i \not| x$ for any i.

But there is some prime p that divides x so that prime was not on our list. Thus our list is not all of the primes, a contradiction. So our assumption

"there are are only finitely many primes" is false. Therefore there are infinitely many primes. $\square$

Definition 1.4. *We say $d \in \mathbb{N}$ is the* **greatest common divisor** *of two integers a and b (that is $d = gcd(a, b)$) if*

- *$d|a$ and $d|b$, and*
- *if $d'|a$ and $d'|b$ then $d'|d$.*

Problem 1.5. *Find the gcd of 18 and 45.*

Factoring is an expensive operation we want an algorithm that is less expensive.

Euclidean Algorithm We will find the gcd(a,b)

first divide a by b	$a = b \cdot q_1 + r_1$	is $r_1 = 0$ then the gcd $= b$
now divide b by r_1	$b = r_1 \cdot q_2 + r_2$	is $r_2 = 0$ then the gcd $= r_1$
now divide r_1 by r_2	$r_1 = r_2 \cdot q_3 + r_3$	is $r_2 = 0$ then the gcd $= r_2$

continue until the remainder is zero.

Example Find the gcd(312, 252).

$$\begin{array}{lcrl} 312 & = & 252(1) & +60 \\ 252 & = & 60(4) & +12 \\ 60 & = & 12(5) & +0 \end{array}$$

Thus the gcd is 12.

Problem 1.6. *Find the gcd(330,1575)*

Theorem 1.7. *Let $a, b \in Z$ and $d = \gcd(a, b)$. Then there exist $x, y \in \mathbb{Z}$ so that*

$$ax + by = d.$$

	gcd(18,45) = 9	18(-2) + 45(1) = 9
So we have	gcd(312, 252) = 12	312(-4) + 252(5) = 12
	gcd(330,1575)= 15	330(??) + 1575(??) = 15

How did I find these answers. First we rewrite the previous calculations.

$$\begin{array}{lcrl|l} 312 & = & 252(1) & +60 & 60 = 312(1) + 252(-1) \\ 252 & = & 60(4) & +12 & 12 = 252(1) + 60(-4) \\ 60 & = & 12(5) & +0 & \end{array}$$

Next we work in reverse.

$$12 = 252(1) + 60(-4) \tag{1}$$
$$12 = 252(1) + (312(1) + 252(-1))(-4) \text{ sub in } 60 = 312(1) + 252(-1) \tag{2}$$
$$12 = 252(1) + 312(-4) + 252(4) \text{ distribute} \tag{3}$$
$$12 = 252(5) + 312(-4) \text{ add like terms} \tag{4}$$

Problem 1.8. *Find x and y so that*

$$330x + 1575y = 15.$$

1.2 Diophantine Equations

Let a, b and $n \in \mathbb{Z}$. The equation

$$ax + by = n \tag{5}$$

has a a solution in integers if and only if $d|n$ where $d = gcd(a, b)$. Moreover, if (x_0, y_0) then

$$x = x_0 - \frac{b}{d}t \tag{6}$$
$$y = y_0 + \frac{a}{d}t \tag{7}$$

is a solution for any $t \in \mathbb{Z}$.

How to find a solution ax+by=d (if d—n where d = gcd(a,b))

1. Find a solution to equation ax+by=d, say (x_0, y_0)
2. So $ax_0 + by_0 = d$ now multiply by $\frac{n}{d}$ to get $a(x_0 * \frac{n}{d}) + b(y_0 * \frac{n}{d}) = n$
3. Use equation (7) to get other answers if desired.

Problem 1.9 (Euler, 1770)**.** *Divide 100 into two summands such that one is divisible by seven and the other is divisible by 11.*

Solution This problem is $100 = 7x + 11y$.

find d = gcd(7,11) = 1

find solution to $1 = 7x + 11y$. I get $1 = 7(-3) + 11(2)$

Multiply by 100 to get $100 = 7(-300) + 11(200)$

it seems this answer is correct but Euler wants positive numbers so let's look for other answers with

$$
\begin{aligned}
x &= -300 - \frac{11}{1}t = -300 - 11t \\
y &= 200 + \frac{7}{1}t = 200 + 7t
\end{aligned}
$$

- To guarantee $x > 0$ we need $-300 - 11t > 0$ thus $t < \frac{300}{11} \approx -27.3$
- To guarantee $y > 0$ we need $200 + 7t > 0$ thus $t > \frac{200}{7} \approx -28.6$

So the only answer is if $t = -28$. So

$$
\begin{aligned}
x &= -300 - 11(-28) = 8 \\
y &= 200 + 7(-27) = 4
\end{aligned}
$$

Therefore $100 = 7(8) + 11(4) = 56 + 44$.

Problem 1.10. *Find x and y so that*

$$330x + 1575y = 15.$$

Problem 1.11 (Mahaviracarya, 850)**.** *There were 63 equal piles of plantain fruit and 7 single fruits. They were divided equally among 23 travelers. What is the number of fruit in each pile?*

Problem 1.12 (Alcuin of York, 775)**.** *One hundred bushels of grain are distributed among 100 persons in such a way that each man receives 3 bushels, each woman receives 2 bushels and each child receives 1/2 bushel. How many men women and children were there?*

Problem 1.13 (Yen Kung, 1372)**.** *We have an unknown number of coins. In piles of 78 coins we are 50 coins short. But in piles of 78 coins we have the right number of coins. How may coins are there?*

Problem 1.14 (Homework - New Yorker)**.** *Six sailors survive a shipwreck and swim to a tiny island where there is nothing but a coconut tree and a monkey. The sailors gather all the coconuts and put them in a big pile under the tree. Exhausted, they agree to wait until the next morning to divide up the coconuts. At one o'clock in the morning, the first sailor wakes. He realizes that he can't trust the others, and decides to take his share now. He divides the coconuts into six equal piles, but there is one left over. He gives that coconut to the monkey, buries his coconuts, and puts the rest of* *the coconuts back under the tree. At two o'clock, the second sailor wakes up. Not realizing that the first sailor has already taken his share, he too divides the coconuts up into six piles, leaving one left over which he gives to the monkey. He then hides his share, and piles the remainder back under the tree. At three o'clock, the third sailor wakes up and carries out the same actions. And so do the fourth fifth and sixth sailor.*

Later in the morning, all the sailors wake up, and try to look innocent. No one makes a remark about the diminished pile of coconuts, and no one decides to be honest and admit that they've already taken their share. Instead, they divide the pile up into six piles, for the seventh time, and find that there is yet again one coconut left over, which they give to the monkey.

How many coconuts were there originally?

2 A Rough Introduction to Modular Mathematics

2.1 Modular Mathematics

A bit of notation. We say d **divides** n if $d = kn$ for some $k]in/Z$ and we write as $d|n$.
Example: We write $3|12$ and we write $3 \not| 13$. If $d|n$ we say d is a divisor of n.

Definition 2.1. *We say $a \equiv b$ mod n if and only if $n|(b-a)$.*

Example: Some simple examples of modular math:

$$3 \equiv 7 \mod 2 \text{ since } 2|(3-7)$$

$$7 \equiv 3 \mod 2 \text{ since } 2|(3-7)$$

$$3 \not\equiv 7 \mod 3 \text{ since } 3 \not|(3-7)$$

$$\text{Find a number } a \text{ so that } a \equiv 47 \mod 13 \ldots$$

Problem 2.2. *Find all numbers a so that*

$$a \equiv 2 \mod 3.$$

Solution Note 5 works $5 \equiv 2 \mod 3$.
Note 8 works $8 \equiv 2 \mod 3$.
Note 11 works $11 \equiv 2 \mod 3$.
Maybe there is a pattern here ... I believe we have all the numbers

$$\{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}.$$

In fact we have

- $0 \equiv 3 \equiv 6 \equiv 9 = \cdots \mod 3$
- $1 \equiv 4 \equiv 7 \equiv 10 = \cdots \mod 3$, and
- $2 \equiv 5 \equiv 8 \equiv 11 = \cdots \mod 3$.

Notice every number (even negatives) are equivalent to either $0, 1$,or 2 mod 3. In fact we have for any number, say 23

$$\begin{array}{r} ?? \quad \text{R } 2 \\ 3 \overline{)23} \end{array}$$

And $23 \equiv 2 \mod 3$. So mod is just remainder with some algebraic properties. In general for mod n where n is an number larger than 1 we will want to reduce the mod to one of the numbers

$$0, 1, 2, 3 \ldots, n-1$$

which are the remainders we can see when dividing by n.

Problem 2.3. *Reduce the following to numbers in the range* $0, 1, 2 \ldots, n-1$.

$$\begin{aligned} 11 &\equiv \underline{\hspace{2cm}} \mod 7 \\ 23 &\equiv \underline{\hspace{2cm}} \mod 14 \\ 14 &\equiv \underline{\hspace{2cm}} \mod 9 \\ -38 &\equiv \underline{\hspace{2cm}} \mod 10 \\ -7 &\equiv \underline{\hspace{2cm}} \mod 8 \\ 14 &\equiv \underline{\hspace{2cm}} \mod 7 \end{aligned}$$

Note this equivalent, "$\equiv$", is like equals. But it is not equals. It has some similarities and because "$\equiv$" satisfies the following three properties we call "$\equiv$" an equivalence relation.

reflexive. $a \equiv a \mod n$

symmetric. $a \equiv b \mod n$ implies $b \equiv a \mod n$, and

transitive. $a \equiv b \mod n$ and $b \equiv c \mod n$ implies $a \equiv c \mod n$.

So equivalence is like equals, but what about the following operations? Note $8 \equiv 2 \mod 3$ and $0 \equiv 3 \mod 3$. Are the following true?

1. $8 + 0 \equiv 2 + 3 \mod 7$
2. $8 \cdot 0 \equiv 2 \cdot 3 \mod 7$
3. $0^2 \equiv 3^2 \mod 7$
4. $2^0 \equiv 2^3 \mod 7$

I get 1, 2 and 3 are true but 4 is false! So equivalence is NOT equals, but it is certainly like it.

Proposition 2.4. *Assume* $a \equiv b \mod n$ *and* $c \equiv d \mod n$*. Then*

- $a + c \equiv b + d \mod n$

- $ac \equiv bd \mod n$ *and*
- $a^e \equiv b^e \mod n$ *for any* $e \in \mathbb{Z}$.

Proof. Since $a \equiv b \mod n$ and $c \equiv d \mod n$ we have that $n|(a-b)$ and $n|(c-d)$. Thus there are $k, l \in \mathbb{Z}$ so that $(a-b) = kn$ and $(c-d) = ln$. Note $(a+c)-(b+d) = (a-b)+(c-d) = kn+ln = (k+l)n$. Thus $n|(a+c)-(b+d)$. Therefore

$$a + c \equiv b + d \mod n.$$

The other two are left for you.

□

2.1.1 Reducing large numbers modulo n

Example: We want to reduce $2^{100} \mod 11$. This is a number larger than the calculator can hold. How can we do it? By repeated squaring we can easily jump to large exponents.

$$\begin{aligned}
2^1 &\equiv 2 \mod 11 \\
2^2 &\equiv 4 \mod 11 \\
2^4 &\equiv 16 \equiv 5 \mod 11 \\
2^8 &\equiv (2^4)^2 \equiv 5^2 \equiv 245 \equiv 3 \mod 11 \\
2^{16} &\equiv 3^2 \equiv 9 \mod 11 \\
2^{32} &\equiv 9^2 \equiv (-2)^2 \equiv 4 \mod 11 \\
2^{64} &\equiv 4^2 \equiv 5 \mod 11
\end{aligned}$$

And then note $100 = 64 + 32 + 4$ so

$$2^{100} = 2^{64}2^{32}2^4 \equiv 5 \cdot 4 \cdot 5 \equiv 20 \cdot 5 \equiv (-2) \cdot 5 \equiv -10 \equiv 1 \mod 11.$$

Problem 2.5. *Reduce the following:*

- $3^{100} \mod 7$*, and*
- $3^{100} \mod 9$.

We have methods even faster then repeated squaring for reducing large numbers modulo n. Here are two useful tools.

Theorem 2.6 (Fermat's Little Theorem)**.** *Let* p *be a prime and* $a \in \mathbb{Z}$ *so that* $gcd(a, p) = 1$ *then*

$$a^{p-1} \equiv 1 \mod p.$$

Corollary 2.7. *Let $n = pq$ where p and q are primes and $a \in \mathbb{Z}$ so that $gcd(a, n) = 1$ then*

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

where $\phi(n) = (p-1)(q-1)$.

Example Let's reduce $3^{100} \mod 7$ again using FLT. Note by FLT $3^6 \equiv 1 \mod 7$. So

$$3^{100} \equiv 3^{6 \cdot 16+4} \equiv (3^6)^{16} 3^4 \equiv (1)^{16} 3^4 \equiv 9^2 \equiv (-2)^2 \equiv 4 \mod 7.$$

Easier than the repeated squaring method.

Example Let's reduce $3^{100} \mod 33$ using the corollary. Why do we need the corollary and why can we not use FLT?

Note by corollary $3^{20} \equiv 1 \mod 33$ since

$$\phi(33) = \phi(3 \cdot 11) = (3-1)(11-1).$$

So

$$3^{100} \equiv 3^{20*5} \equiv (3^{20})^5 \equiv (1)^5 \mod 33.$$

Again simpler and easier than the repeated squaring method.

Problem 2.8. *Reduce the following.*

1. $2^{2014} \mod 31$
2. $3^{2014} \mod 23$
3. $3^{130} \mod 55$
4. *Find k so that $3k \equiv 1 \mod 31$*
5. *Find k so that $7k \equiv 1 \mod 33$*

3 Chinese Remainder Theorem

The problem

$$n = r_i \mod p_i \tag{8}$$

for i = 1,2,3,...,n

The equation has a solution if for all $i \neq j$ we have

$$\gcd(p_i, p_j) = 1.$$

The answer is

$$n = \frac{p}{p_1}k_1r_1 + \frac{p}{p_2}k_2r_2 + + \cdots + \frac{p}{p_n}k_nr_n$$

where $p = p_1p_2\cdots p_n$ and k_i is the solution to

$$\frac{p}{p_i}k_i \equiv 1 \mod p_i.$$

And any number equivalent to $n \mod p$ is also an answer.

So example find n so that

$n = 1 \mod 2$
$n = 2 \mod 3$
$n = 3 \mod 7$

Solution Note $p = p_1p_2p_3 = 2 \cdot 3 \cdot 7 = 42$. Now we compute each k_i

k_1**:**

$$\frac{p}{p_1}k_1 \equiv 1 \mod p_1 = \frac{42}{2}k_1 \equiv 1 \mod 2 = 21k_1 \equiv 1 \mod 2 = (1)k_1 = 1 \mod 2$$

So $k_1 = 1$.

k_2**:**

$$\frac{p}{p_2}k_2 \equiv \frac{42}{3}k_1 \mod 3 \equiv 14k_1 \equiv (2)k_1 = 1 \mod 3$$

Trying all the possibilities for $k_2 = \{0, 1, 2, \}$ and we get $k_2 = 2$.

k_3**:**

$$\frac{p}{p_3}k_3 \equiv \frac{42}{7}k_1 \mod 7 \equiv \text{‘}6k_1 \equiv 1 \mod 7$$

Try all possible remainders for k_3 we get $k_3 = 6$.

S0 the answer is

$$n = \frac{p}{p_1}k_1r_1 + \frac{p}{p_2}k_2r_2 + \frac{p}{p_3}k_3r_3$$

$$= \frac{42}{2}(1)(1) + \frac{42}{3}(2)(2) + \frac{42}{7}(6)(3)$$
$$= 21 + 56 + 108 = 185$$

And for the smallest positive answer I get $n = 17$.

For you all.

Problem 3.1 (Ancient Chinese Problem)**.** *A band of 17 pirates stole a sack of gold. When they tried to divide the gold equally between the pirates there were 3 gold coins remaining. An brawl ensued; on pirate died. So the pirates tried to divide the gold equally again. Again it did not come out evenlt. There were 10 gold coins remaining. Another brawl ensued; another dead pirate. Another attempt to divide the gold and now the gold was divided evenly.*

How much gold was there?

4 Cryptography

We will take the alphabet and perform some math on it to disguise the message. Here is our alphabet.

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

So he will take a message like

plainText =

H	E	L	L	O	Z	E	D
07	04	11	11	14	25	04	03

We the **encipher** the plainText: cipherText = scramble the plainText.

We the **decipher** the cipherText: plainText = unscramble the cipherText.

We will analyze two methods used some of the most powerful entities in history: Caesar and modern internet banking.

4.0.2 Caesar's Cipher

Back to our message.

plainText =

H	E	L	L	O	Z	E	D
07	04	11	11	14	25	04	03

We encipher by applying the Caesar's cipher "+3" (mod 26).

cipherText =

10	07	14	14	17	02	07	06
K	H	O	O	R	C	H	G

To decipher we apply "-3" (mod 26).

plainText =

07	04	11	11	14	25	04	03
H	E	L	L	O	Z	E	D

4.0.3 What professor's bank uses to protect his pennies

The Caesar cipher is of interest for an introductory ciphering technique. However, it is a bit too simple to be of use today. In fact it was decrypted by Caesar's enemies and abandoned by Caesar himself. The next cipher method we will learn is called RSA and is robust enough that is used by modern banks today.

RSA contains a few elements in modern cryptography:

- We assume our enemy hackers will know what technique we are using.
- We will publish open for all to see the method and keys to encipher a message. So anyone can encipher to send to us. But only we should be able to decipher the message.

SETUP: We will have more numbers involved: n, p, q, e and d

- We pick two primes p and q.
- Compute n=pq; n is our modulus.
- We pick e, the enciphering exponent so that $\gcd(e, \phi(n)) = 1$.
- We compute d, the deciphering exponent so that $de \equiv 1 \mod phi(n)$.

public key: (n, e) private key: (n, e)

TO ENCIPHER: Break the plainText into blocks $P_1, P_2, P_3, \cdots$ where the max size of the $P_i < n$. Then

$$C = P^e \mod n.$$

is the cipherText.

TO DECIPHER:

$$P = C^d \mod n.$$

is the plainText.

Example SETUP:

- We pick two primes p=3 and q=11.
- Compute n=pq = 33. Note n¿26 so we can decode a single letter per block.
- We pick $e = 7$, note $\gcd(7, \phi(33)) = 1$. I think, wait what was that $\phi(33)$ again?

- We compute $d = 3$. Note $de \equiv 3 \cdot 7 \equiv 1 \mod phi(n)$.

public key: (33, 7) private key: (33, 3)

TO ENCIPHER: We can use our favorite message

plainText =

H	E	L	L	O	Z	E	D
07	04	11	11	14	25	04	03

And our blocks will be $P_1 = 07, P_2 = 04, P_3 = 11, \cdots$

So to encipher

$$C_1 \equiv P_1^e \equiv 07^7 \equiv \cdots \equiv 28 \mod 33$$

$$C_2 \equiv P_2^e \equiv 04^7 \equiv \cdots \equiv 16 \mod 33$$

cipherText =

28	16	11	11	20	31	16	9

TO DECIPHER: We use $C_1 = 28, C_2 = 16, C_3 = 11, \cdots$ and the formula

$$P = C^d \mod n.$$

$$P_1 \equiv C_1^d \equiv 28^3 \equiv (-5)^3 \equiv -125 \equiv -125 + 4 * 33 \equiv 07 \mod 33$$

$$P_2 \equiv C_2^d \equiv 16^3 \equiv \cdots \equiv 04 \mod 33$$

Problem 4.1. *1. Make your own RSA setup. Make sure to pick to primes so that $n = pq > 26$.*

2. Compute n, d and e.

3. Encipher your favorite message. Mine is "Math is fun".

4. Decipher it as well.

5 Chinese Remainder Theorem and Pell's Equation

We don't seem to have time, but feel free to stop by and ask ...