Recap/Exercise

(1) Find all the units (elements of a ring w/ multiplicative inverse) of $\mathbb{Z}_{10}$ (the ring of integers modulo 10 (with operations addition and multiplication modulo 10))

we have seen: m is a zero divisor modulo $n \iff \gcd(m,n) > 1$

m is a unit modulo $n \iff \gcd(m,n) = 1$

$\Rightarrow U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$

$U(R)$ = set of units of the ring R. This set forms a group under multiplication.

If $U(R) = R \setminus \{0\}$ then R is called a division ring.

If it's commutative then it's called a field.

(2) Show that $U(\mathbb{Z}_{10})$ and $U(\mathbb{Z}_8)$ are not isomorphic

$U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$

So the two groups have the same order. They're both commutative.

However, in $U(\mathbb{Z}_{10})$: $\text{ord}_{U(\mathbb{Z}_{10})}(3) = 4$ as $3^2 = 9 \neq 1$

$3^3 = 27 = 7 \neq 1$

$3^4 = 81 = 1$

while all elements in $U(\mathbb{Z}_8)$ have order 2: $3^2 = 16 = 1 \pmod 8$

$5^2 = 25 = 1 \pmod 8$

$7^2 = 49 = 1 \pmod 8$

An isomorphism preserves the order of the elements, therefore $U(\mathbb{Z}_{10}) \not\cong U(\mathbb{Z}_8)$.

(3) Compute $|U(\mathbb{Z}_{100})|$ (from exam paper 18-19)

listing all elements is a bit too long... Euler's totient function!

(4) Compute 4^{2019} in $\mathbb{Z}_{11}$

Lecture 13

2.4 More number theory. Euler's function and Euler's thm.

Recall that the division algorithm & elementary properties of factorisation of integers give an algorithm to find the gcd of any given pair of numbers. This is called the Euclidean algorithm and works as follows:

to compute $\gcd(a,b)$

write

$$a = bq_1 + r_1 \quad \text{with } 0 \le r_1 < b$$

if $r_1 = 0$ then b is the desired gcd

if $r_1 > 0$ then write $b = r_1 q_2 + r_2$ with $0 \le r_2 < r_1$

⋮

write $r_{k-2} = r_{k-1} \cdot q_k + r_k$ with $0 \le r_k < r_{k-1}$

when $r_k = 0$ then r_{k-1} is the desired gcd.

Example: $\gcd(2019, 522)$

$2019 = 522 \cdot 3 + 447$

$522 = 447 \cdot 1 + 75$

$447 = 75 \cdot 5 + 72$

$75 = 72 \cdot 1 + 3$

$72 = 24 \cdot 3$ (remainder is 0, penultimate remainder is gcd)

This algorithm also gives us a method to write gcd of two numbers as a "linear combination" of these numbers.

This works by going backwards in the Euclidean algorithm expressing the various remainders as l.c. of the other integers involved.

Example (from exam paper 2018-19) Find $\gcd(33,56)$ and find integers m,n such that

$$1 = 33m + 56n$$

Euclidean algorithm:

(1) $56 = 33 \cdot 1 + 23$

(2) $33 = 23 \cdot 1 + 10$

(3) $23 = 10 \cdot 2 + 3$

(4) $10 = 3 \cdot 3 + 1$

$3 = 3 \cdot 1$

(*)

$1 = 10 - 3 \cdot 3$ in (3) solve for 3: $3 = 23 - 10 \cdot 2$ and use in (*)

$1 = 10 - (23 - 10 \cdot 2) \cdot 3$ collect common terms

$1 = 10 \cdot 7 - 23 \cdot 3$ use an expression for 10 from (2)

$1 = (33 - 23) \cdot 7 - 23 \cdot 3$ collect..

$1 = 33 \cdot 7 - 23 \cdot 10$ use an expression for 23 from (1)

$1 = 33 \cdot 7 - (56 - 33) \cdot 10$

$1 = 33 \cdot 17 - 56 \cdot 10$

$m = 17$, $n = -10$ are the desired integers.

The following hold:

- The gcd of integers a, b (both nonzero) can be expressed as a linear combination of a and b:

$$\gcd(a,b) = am + bn \quad \text{for some } m,n \in \mathbb{Z}$$

- In particular, if a and b are integers, then $\gcd(a,b)=1$ if and only if

$\exists$ m,n integers such that $am+bn=1$

We know now how to find the gcd of two integers — and in particular to check whether two integers are coprime. But what if we only want to know how many coprime integers (positive) there are which are smaller than our given number? (For instance, to know how many elts are units modulo a given number).

First note that if $n=p$ is a prime, the answer is easy:

$$\#\{m \leq p \text{ such that } \gcd(m,p)=1\} = p-1$$

Definition (Euler's totient function)

For each integer >1 let $\varphi(n)$ denote the number of positive integers that are less than n and relatively prime with n (that is, their gcd with n is 1). Also, let $\varphi(1)=1$.
We call this function Euler's phi function or Euler's totient function.

For instance $\varphi(5)=4$ and $\varphi(p)=p-1$ for any prime number

$\varphi(8)=4$
$\varphi(10)=4$ } (from example at the beginning)

This function satisfies some properties which help us reduce the calculations to small numbers:

(a) • if p is a prime then $\varphi(p^r) = p^r - p^{r-1}$

(b) • if p and q are primes then $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$

(c) • In general, if m,n are such that $\gcd(m,n)=1$ then $\varphi(mn) = \varphi(m)\varphi(n)$

Going back to our question: $|U(\mathbb{Z}_{100})| = ?$

write $100 = 2^2 \cdot 5^2$ $\rightsquigarrow$ $|U(\mathbb{Z}_{100})| = \varphi(100) \overset{(c)}{=} \varphi(2^2)\varphi(5^2) \overset{(a)}{=} (2^2-2^1)(5^2-5^1)$

$= (4-2)(25-5)$

$= 2 \cdot 20 = 40$

Using the fact that $|U(\mathbb{Z}_n)| = \varphi(n)$ and reasoning as in Fermat's little theorem, one can show that the following generalisation holds:

Thm (Euler's theorem) If n is a positive integer and $\gcd(a,n)=1$ then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Example Find the remainder of 7^{1000} when divided by 24.

$\updownarrow$

$7^{1000} \bmod 24$.

Note: $\gcd(7,24)=1$ so $7^{\varphi(24)} \equiv 1 \bmod 24$
$\varphi(24) = \varphi(3)\varphi(8) = 2 \cdot 4 = 8$
$\rightsquigarrow$ $7^8 \equiv 1 \bmod 24$