Week 4, lecture 2:
Euler Phi function
MA180/185/190 Algebra

Angela Carnevale

More on prime numbers

Euler's Phi function

Facts about prime numbers

Recall that an integer $p > 1$ is called **prime** if its only divisors are 1 and p itself. If p is a prime and a and b are any integers, then

- either p divides a, or $\gcd(a, p) = 1$;
- if $p | a \cdot b$ then $p | a$ or $p | b$.

unique up to reordering of the factors

Prime numbers are the "building blocks" of the integers:

Fundamental Theorem of Arithmetic

Each integer $n > 1$ has a prime power factorisation

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

where $p_1, \ldots, p_k$ are distinct primes and $e_1, \ldots, e_k$ are positive integers.

An integer $n > 1$ that is not a prime is called a **composite** number.

Fermat's little theorem

The following result is helpful when computing powers of some integer modulo a prime number.

Fermat's little theorem

Let p be a prime and let $a \not\equiv 0 \pmod{p}$ be an integer. Then

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

Note. An easy consequence of this theorem is that $a^p \equiv a \pmod{p}$ if a is any integer and p is a prime.

Fermat's little theorem: proof

Fermat's little theorem

Let p be a prime and let $a \not\equiv 0 \pmod{p}$ be an integer. Then

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

Proof. Let a and p be as in the statement of the theorem.

Consider the numbers: $a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a$

Intermediate claim: $a, 2a, \ldots (p-1)a$ are all DISTINCT modulo p

suppose instead that we find i and j such that

$$i \cdot a \equiv j \cdot a \pmod{p}$$

that is, $(i \cdot a - j \cdot a)$ is divisible by p. But then this tells us that

$p \mid a \cdot (i-j)$ By the properties of primes, this means

either $p \mid a$ or $p \mid (i-j)$ but we know by hypothesis that $p \nmid a$

Fermat's little theorem: proof

Fermat's little theorem

Let p be a prime and let $a \not\equiv 0 \pmod{p}$ be an integer. Then

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

so $p \mid (i-j)$ so $i \equiv j \mod p$ and because they are both $< p$ they have to be equal. This proves our intermediate claim.

So the product $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots (p-1) \pmod{p}$

that is: $1 \cdot 2 \cdot 3 \cdot \ldots a^{p-1} \equiv 1 \cdot 2 \cdot 3 . (p-1) \pmod{p}$

So $a^{p-1} \equiv 1 \pmod{p}$

Fermat's little theorem: example

Example. Find $x \in \mathbb{Z}_{19}$ such that $x \equiv 2^{68} \pmod{19}$.

$\gcd(2,19)=1$ and 19 is a prime so we can apply FLT.

$$2^{18} \equiv 1 \pmod{19}$$

By the Remainder theorem $68 = 3\cdot 18 + 14$ so:

$$2^{68} = 2^{18\cdot 3+14} = (2^{18})^3 \cdot 2^{14}. \quad \text{Now mod } 19:$$

$$\underbrace{(2^{18})^3}_{\equiv 1 \text{ by FLT}} \cdot 2^{14} \equiv (2^5)^2 \cdot 2^4 \equiv (32)^2 \cdot 16 \equiv (13)^2 \cdot 16$$

$$\equiv 169 \cdot 16 \equiv (-2)\cdot(-3) \equiv 6 \mod 19$$

Exercise. Find the least non-negative integer x such that $x \equiv 3^{91} \pmod{23}$.

More on prime numbers

Euler's Phi function

Euler's Phi function

We have seen that given a modulus m, the numbers in $\mathbb{Z}_m$ that are **coprime** to m are the only ones which have **inverses** modulo m.

Definition (Euler's Phi function)

Let m be a positive integer. We define $\Phi(m)$ to be the number of integers in $\mathbb{Z}_m$ that are coprime to m.

Examples.

- $\Phi(6) = 2$ $\quad \cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5$
- $\Phi(10) = 4$ $\quad \cancel{0}\ 1\ \cancel{2}\ 3\ \cancel{4}\ \cancel{5}\ \cancel{6}\ 7\ \cancel{8}\ 9$
- $\Phi(p) = p - 1$ for any prime number p.

Computing Euler's Phi function

To compute Euler's Phi function of composite numbers, we can use the following useful facts:

- If m and n are **coprime**, then

$$\boxed{\Phi(mn) = \Phi(m)\Phi(n)}$$

$10 = 2 \cdot 5$ so $\phi(10) = \phi(2) \cdot \phi(5) = 1 \cdot 4 = 4$

Computing Euler's Phi function

To compute Euler's Phi function of composite numbers, we can use the following useful facts:

- If m and n are **coprime**, then

$$\boxed{\Phi(mn) = \Phi(m)\Phi(n)}$$

- If p is a **prime number** and e is a positive integer, then

$$\boxed{\Phi(p^e) = p^e - p^{e-1}}$$

$$\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$$

Computing Euler's Phi function

To compute Euler's Phi function of composite numbers, we can use the following useful facts:

- If m and n are **coprime**, then

$$\boxed{\Phi(mn) = \Phi(m)\Phi(n)}$$

- If p is a **prime number** and e is a positive integer, then

$$\boxed{\Phi(p^e) = p^e - p^{e-1}}$$

Example. How many numbers in $\mathbb{Z}_{26}$ have an inverse?

Euler's Phi function and powers

Theorem

If $\gcd(a, m) = 1$ then

$$a^{\Phi(m)} \equiv 1 \pmod{m}.$$

Note. In the special case in which m is a prime number, this is Fermat's little theorem.

Example. Determine the last two digits of 3^{176}.