

20.3. Proof of Euler's formula. I will prove Euler's formula 20.8 using groups and rings. As an application of the group theory behind the numerical formula we will see that 561 is a pseudoprime.

First, suppose that n is a power of a prime number p :

$$n = p^k$$

For example, $n = 81 = 3^4$. Then Theorem 20.5 says that the units of \mathbb{Z}_{p^k} are those numbers which are relatively prime to p^k . But this is the same as saying that they are not divisible by p . This is the complement of the subset

$$p\mathbb{Z}_{p^k} = \{0, p, 2p, 3p, \dots, p^k - p\}$$

In the example, this is

$$3\mathbb{Z}_{81} = \{0, 3, 6, 9, 12, \dots, 78\}$$

This is a subgroup of \mathbb{Z}_{p^k} of index p . So

$$|p\mathbb{Z}_{p^k}| = p^{k-1}$$

The elements left over are the units:

$$|U(\mathbb{Z}_{p^k})| = p^k - p^{k-1} = (p-1)p^{k-1} = \left(\frac{p-1}{p}\right) p^k$$

So, Euler's formula holds when n is a power of a prime.

Any positive integer n is a product of powers of distinct primes and we have two theorems.

Theorem 20.9. *If R, S are rings with unity 1 then $(1, 1)$ is unity in $R \times S$ and*

$$U(R \times S) = U(R) \times U(S)$$

Note that $R \times S$ is a product of rings and $U(R) \times U(S)$ is a product of groups.

This is an example of a theorem in which all of your knowledge and effort should be put into understanding what it says because the proof is completely trivial.

Corollary 20.10. *If R_1, \dots, R_n are rings with unity then*

$$U(R_1 \times R_2 \times \dots \times R_n) = U(R_1) \times U(R_2) \times \dots \times U(R_n)$$

The theorem says this is true for $n = 2$. For larger n it follows by induction in the standard way.

Next we need a theorem which we may have already proven:

Theorem 20.11. *If n, m are relatively prime then we have a ring isomorphism:*

$$\phi : \mathbb{Z}_{nm} \xrightarrow{\cong} \mathbb{Z}_n \times \mathbb{Z}_m$$

Proof. The ring homomorphism ϕ is given by

$$\phi(x) = (x \pmod n, x \pmod m)$$

This is a ring homomorphism because n and m divide nm :

$$\phi(x +_{nm} y) = (x +_n y, x +_m y) = (x, x) + (y, y) = \phi(x) + \phi(y)$$

$$\phi(xy) = (xy, xy) = (x, x)(y, y) = \phi(x)\phi(y)$$

Let's look at just the first step:

$$x +_{nm} y \equiv x +_n y \pmod n$$

This is because both numbers are congruent to $x + y$ modulo n .

To see that ϕ is a bijection, use the Euclidean algorithm as I explained already twice. \square

Instead of writing an arbitrary number, we will take

$$n = 360 = 8 \cdot 9 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$$

Then we have an isomorphism of rings:

$$\mathbb{Z}_{360} = \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$

which gives an isomorphism of groups:

$$U(\mathbb{Z}_{360}) = U(\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5) = U(\mathbb{Z}_8) \times U(\mathbb{Z}_9) \times U(\mathbb{Z}_5)$$

Counting numbers of elements we get

$$\begin{aligned} \phi(2^3 \cdot 3^2 \cdot 5) = |U(\mathbb{Z}_{360})| &= |U(\mathbb{Z}_8)| \cdot |U(\mathbb{Z}_9)| \cdot |U(\mathbb{Z}_5)| = (8-4)(9-3)(5-1) \\ &= 360 \left(\frac{2-1}{2}\right) \left(\frac{3-1}{3}\right) \left(\frac{5-1}{5}\right) = 96 \end{aligned}$$

Although the group of units in \mathbb{Z}_{360} has order 96, we can conclude from the group formula that $g^{12} = e$ for every $g \in U(\mathbb{Z}_{360})$. The reason is that

$$g = (a, b, c) \in U(\mathbb{Z}_8) \times U(\mathbb{Z}_9) \times U(\mathbb{Z}_5)$$

So, $a^4 = e, b^6 = e, c^4 = e$. (In fact $a^2 = e$ since $1^2 = 3^2 = 5^2 = 7^2 = 1$ in \mathbb{Z}_8 .)

Do the same for $n = 561 = 3 \cdot 11 \cdot 17$ and show that:

$$a^{560} \cong 1 \pmod{561}$$

for all integers a relatively prime to 561.

Definition 20.12. A positive integer n is called a pseudoprime or Carmichael number if it has the property that $a^{n-1} \cong 1 \pmod n$ for all integers a relatively prime to n .

There are an infinite number of pseudoprimes and the smallest one is 561.

What is next?

After the quiz, we have three more topics which I want to cover to complete the circle of ideas.

- (1) Finite fields (also called *Galois fields*). The main results are:
 - (a) The number of elements in a finite field is a power of a prime: $|GF| = p^k$. And conversely, for any power of any prime, there is a unique Galois field with this number of elements. Usually we use $GF(2^8)$.
 - (b) The group of units is a cyclic group of order $p^k - 1$.
We need polynomial rings (sections 22,23) to understand the structure of finite fields (section 33).
- (2) Finite simple groups of “Lie type” are constructed out of the finite fields. These account for most of the finite simple groups.
- (3) Extensions All finite groups are iterated extensions of simple groups. I will explain some of this very rich theory if I have time.