

# MATH 136—HOMEWORK 5

Ricardo J. Acuña

(862079740)

1 Evaluate  $\left(\frac{31}{641}\right)$ .

$$\sqrt{31} \approx 5.5677643628300215 < 6$$

So, we check if 31 is divisible by every prime less than 6:

$$31 = 15 \cdot 2 + 1$$

$$31 = 10 \cdot 3 + 1$$

$$31 = 6 \cdot 5 + 1$$

No, so 31 is prime.

$$\sqrt{641} \approx 25.3179778023443 < 26$$

So, we check if 641 is divisible by every prime less than 26:

$$641 = 320 \cdot 2 + 1$$

$$641 = 213 \cdot 3 + 2$$

$$641 = 128 \cdot 5 + 1$$

$$641 = 91 \cdot 7 + 4$$

$$641 = 58 \cdot 11 + 3$$

$$641 = 49 \cdot 13 + 4$$

$$641 = 37 \cdot 17 + 12$$

$$641 = 33 \cdot 19 + 14$$

$$641 = 27 \cdot 23 + 20$$

No, so 641 is prime.

$$\left(\frac{31}{641}\right)\left(\frac{641}{31}\right) = (-1)^{\frac{31-1}{2} \frac{641-1}{2}}$$

$$\implies \left(\frac{31}{641}\right) = (-1)^{\frac{31-1}{2} \frac{641-1}{2}} \left(\frac{641}{31}\right) = (-1)^{15 \cdot 320} \left(\frac{641}{31}\right) = (-1)^{2 \cdot (15 \cdot 160)} \left(\frac{641}{31}\right) = \left(\frac{641}{31}\right)$$

$$641 = 20 \cdot 31 + 21 \implies \left(\frac{31}{641}\right) = \left(\frac{21}{31}\right) = \left(\frac{3 \cdot 7}{31}\right) = \left(\frac{3}{31}\right) \left(\frac{7}{31}\right)$$

$$\left(\frac{3}{31}\right) = (-1)^{\frac{3-1}{2} \frac{31-1}{2}} \left(\frac{31}{3}\right) = (-1)^{1 \cdot 15} \left(\frac{31}{3}\right) = -\left(\frac{31}{3}\right)$$

$$31 = 10 \cdot 3 + 1 \implies \left(\frac{3}{31}\right) = -\left(\frac{1}{3}\right) = -\left(\frac{1^2}{3}\right) = -1$$

$$\left(\frac{7}{31}\right) = (-1)^{\frac{7-1}{2} \frac{31-1}{2}} \left(\frac{31}{7}\right) = (-1)^{3 \cdot 15} \left(\frac{31}{7}\right) = -\left(\frac{31}{7}\right)$$

$$31 = 4 \cdot 7 + 3 \implies \left(\frac{31}{7}\right) = \left(\frac{3}{7}\right) \equiv 3^{\frac{7-1}{2}} \equiv 3^3 \equiv 27 \equiv 3 \cdot 7 + 6 \equiv 6 \equiv -1 \pmod{7}$$

$$\implies \left(\frac{7}{31}\right) = -1 \cdot -1 = 1$$

$$\implies \left(\frac{31}{641}\right) = -1 \cdot 1 = -1$$

2 Show that if  $p$  is an odd prime (bigger than 3) then

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12} \\ -1, & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

pf.

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{3}\right) = (-1)^{1 \cdot \frac{p-1}{2}} \left(\frac{p}{3}\right) \text{ and Euler's Criterion}$$

$$\Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) \equiv (-1)^{\frac{p-1}{2}} p^{\frac{3-1}{2}} \pmod{3} \equiv (-1)^{\frac{p-1}{2}} p^1 \pmod{3} \equiv (-1)^{\frac{p-1}{2}} p \pmod{3}$$

We need to check the possibilities for the remainder  $r$ , of  $p$  when divided by 12.

$$\phi(12) = \phi(2^2 \cdot 3) = \phi(2^2) \cdot \phi(3) = 2^{2-1}(2-1) \cdot (3-1) = 4$$

So, there are only 4 numbers coprime to 12.

We know  $r \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ .  $r$  can't be 0, since  $p$  is prime.  $1^{\phi(12)} = 1 \pmod{12}$  so 1 works. Now,  $p$  is prime so it's not divisible by 2 or 3, so  $p$  can't be congruent modulo 12 to 4, 6, 8, and 10. Now, we need to check the following for completeness.

$$5^{\phi(12)} = 5^4 = 625 = 52 \cdot 12 + 1 \equiv 1 \pmod{12}$$

$$7^{\phi(12)} = 7^4 = 2401 = 200 \cdot 12 + 1 \equiv 1 \pmod{12}$$

$$11^{\phi(12)} = 11^4 = 14641 = 1220 \cdot 12 + 1 \equiv 1 \pmod{12}.$$

$\phi(12) = 4$  together with  $r^{\phi(12)} \equiv 1 \pmod{12} \iff \gcd(r, 12) = 1$  tells us we are done. We found the four, relatively prime numbers to 12, that are less than 12. And, any prime larger than 3 will be congruent to them.

Now  $11 = 12 - 1 \equiv -1 \pmod{12}$  and  $7 = 12 - 5 \equiv -5 \pmod{12}$

So  $p$  is congruent to  $\pm 1$  or  $\pm 5$  modulo 12.

$$p \equiv 1 \pmod{12} \Rightarrow p = 12 \cdot m + 1$$

$$\Rightarrow \left(\frac{3}{p}\right) \equiv (-1)^{\frac{12 \cdot m + 1 - 1}{2}} (12 \cdot m + 1) \equiv (-1)^{2 \cdot 3m} (1) \equiv 1 \pmod{3}$$

$$p \equiv -1 \pmod{12} \Rightarrow p = 12 \cdot m - 1$$

$$\Rightarrow \left(\frac{3}{p}\right) \equiv (-1)^{\frac{12 \cdot m - 1 - 1}{2}} (12 \cdot m - 1) \equiv (-1)^{6 \cdot m - 1} (-1) \equiv (-1)^{odd} (-1) \equiv 1 \pmod{3}$$

$$p \equiv 5 \pmod{12} \Rightarrow p = 12 \cdot m + 5$$

$$\Rightarrow \left(\frac{3}{p}\right) \equiv (-1)^{\frac{12 \cdot m + 5 - 1}{2}} (12 \cdot m + 5) \equiv (-1)^{6 \cdot m + 2} (5) \equiv (-1)^{even} (-2 \cdot 3 + 5) \equiv (1)(-1) \equiv -1 \pmod{3}$$

$$p \equiv -5 \pmod{12} \Rightarrow p = 12 \cdot m - 5$$

$$\Rightarrow \left(\frac{3}{p}\right) \equiv (-1)^{\frac{12 \cdot m - 5 - 1}{2}} (12 \cdot m - 5) \equiv (-1)^{6 \cdot m - 3} (-5)$$

$$\equiv (-1)^{3(2 \cdot m - 1)} (2 \cdot 3 - 5) \equiv (-1)^{odd} (1) \equiv -1 \pmod{3}$$

So, if  $p > 3$  and  $p$  is prime.

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12} \\ -1, & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

■

**3** Find all positive integers  $n$  for which  $\phi(n) = 6$ . Show that these are the only  $n$  for which this holds.

Pf.

$$\phi(n) = 6 \text{ and } n \in \mathbb{N}.$$

Either,  $n$  is prime or not.

(I)  $n$  is prime:

$$\phi(n) = n - 1 \implies n - 1 = 6 \implies n = 7$$

(II)  $n$  isn't prime:

So,  $n$  it's composite—i.e.  $n = p_0^{m_0} p_1^{m_1} \dots p_k^{m_k}$  where  $p_i$  is prime, and  $m_i \geq 0$ , and  $k$  finite.

$$\phi(\cdot) \text{ is multiplicative. } \implies \phi(n) = \phi(p_0^{m_0} p_1^{m_1} \dots p_k^{m_k}) = p_0^{m_0-1}(p_0-1) p_1^{m_1-1}(p_1-1) \dots p_k^{m_k-1}(p_k-1) = 6 = 2 \cdot 3$$

Part of the product corresponds to 2 and part to 3, since  $\phi(\cdot)$  is multiplicative.

So, let's consider up to rearrangement

$$\phi(s) = p_0^{m_0-1}(p_0-1) \dots p_r^{m_r-1}(p_r-1) = 2 \text{ and } \phi(t) = p_{r+1}^{m_{r+1}-1}(p_{r+1}-1) \dots p_k^{m_k-1}(p_k-1) = 3$$

Since 2 is prime, there's only one  $p_i$  in the product and ( $[m_i-1=0$  and  $p_i-1=2]$  or  $[p_i-1=1$  and  $p_i^{m_i-1}=2]$ )

$$m_i-1=0 \text{ and } p_i-1=2 \implies p_i=3 \implies s=3$$

$$p_i-1=1 \text{ and } p_i^{m_i-1}=2 \implies p_i=2 \text{ and } 2^{m_i-1}=2^1 \implies m_i-1=1 \implies m_i=2 \implies s=2^2=4$$

Of course we need to consider, values of  $\phi(\cdot)$  where it is equal to 1.  $\phi(1) = 1$ , by convention.

$$\text{For } p \text{ prime, } \phi(p) = 1 \implies p-1=1 \implies p=2.$$

$$\text{For a composite } l = q_0^{c_0} \dots q_a^{c_a}, \phi(l) = q_0^{c_0-1}(q_0-1) \dots q_a^{c_a-1}(q_a-1) = 1$$

All, the  $c_i$  must be 1, because if they weren't their product of powers of primes would have a term bigger than 1.

$$\text{So, } \phi(l) = q_0^0(q_0-1) \dots q_a^0(q_a-1) = (q_0-1) \dots (q_a-1) = 1$$

By the previous logic, one of the terms  $q_i$  must be 2. But, this means that  $1 = (q_0-1) \dots (2-1) \dots (q_a-1)$ , that can't happen, as you'd have a product of primes bigger than 2 minus 1, equaling 1. So,  $l$  isn't composite.

$$\text{So, } \phi(3) = \phi(4) = \phi(3)\phi(2) = \phi(6) = 2.$$

$$\text{Note, } \phi(8) \neq \phi(4)\phi(2) = 2 \text{ as } \gcd(4, 2) = 2.$$

Since 3 is prime, there's only one  $p_j$  in the product

$$\text{and } ([m_j-1=0 \text{ and } p_j-1=3] \text{ or } [p_j-1=1 \text{ and } p_j^{m_j-1}=3])$$

$$m_j=0 \text{ and } p_j-1=3 \implies p_j=4, \text{ but } p_j \text{ is prime so it can't happen.}$$

$$p_j-1=1 \text{ and } p_j^{m_j-1}=3 \implies p_j=2 \implies 2^{m_j-1}=3 \text{ is false, so } \nexists n \in \mathbb{N} : \phi(n) = 3$$

However, we have  $\forall n, k \in \mathbb{N} : \phi(n^k) = n^{k-1}\phi(n)$ , where  $n$  prime.

So, for each we can check,

$$\phi(3) = 2 \implies 3\phi(3) = \phi(3^2) = \phi(9) = 3 \cdot 2 = 6$$

$$\phi(4) = 2 \text{ gives no information as } 4 \text{ isn't a power of } 3.$$

$$\text{And of course we can multiply by 2 as } \gcd(3, 2) = 1.$$

$$\text{So, } \phi(18) = 6$$

Finally, we need to consider multiplying by 2 case (I).

$$\text{This gives } \phi(14) = 6.$$

Summing up  $n \in \{7, 9, 18, 14\} \subset \mathbb{N}$ , and the list is exhaustive by the arguments above.

■

4 Show that for  $n$  a positive integer,

$$\phi(2n) = \begin{cases} \phi(n), & \text{if } n \text{ is odd} \\ 2\phi(n), & \text{if } n \text{ is even} \end{cases}$$

Pf.

(I)  $n$  is odd

$n$  is odd and 2 is prime  $\implies \gcd(n, 2) = 1$

$$\implies \phi(2n) = \phi(2)\phi(n) = (2-1)\phi(n) = \phi(n)$$

(II)  $n$  is even

$$\implies \exists k \in \mathbb{Z} : n = 2^m k, m \geq 1, \text{ and } k \text{ odd.}$$

$$\implies 2n = 2 \cdot 2^m k = 2^{m+1} k$$

2 is prime and  $k$  is odd  $\implies \gcd(k, 2^{m+1}) = 1$

$$\implies \phi(2^{m+1} k) = \phi(2^{m+1})\phi(k)$$

$\forall n, k \in \mathbb{N} : \phi(n^k) = n^{k-1}\phi(n)$ , where  $n$  prime.

2 is prime  $\implies \phi(2^{m+1}) = 2^{m+1-1}(2-1) = 2^m$

$$\implies \phi(n) = 2^m \phi(k)$$

If  $m = 1$ , we're done.

If  $m > 1$ , then  $\phi(n) = 2 \cdot 2^{m-1}(2-1)\phi(k) = 2 \cdot 2^{m-1}\phi(2)\phi(k) = 2\phi(2^m)\phi(k)$

2 is prime and  $k$  is odd  $\implies \gcd(k, 2^m) = 1 \implies \phi(2^m)\phi(k) = \phi(2^m k) = \phi(n)$

$$\implies \phi(n) = 2\phi(n)$$

So,

$$\phi(2n) = \begin{cases} \phi(n), & \text{if } n \text{ is odd} \\ 2\phi(n), & \text{if } n \text{ is even} \end{cases}$$

■

5 Which positive integers have an odd number of positive divisors? Explain why.