MATH 136—HOMEWORK 5

Ricardo J. Acuña

(862079740)

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

pf:

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

$\implies \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) \equiv (-1)^{\frac{p-1}{2}} p^{\frac{3-1}{2}} (\text{mod } 3) \equiv (-1)^{\frac{p-1}{2}} p^1 (\text{mod } 3) \equiv (-1)^{\frac{p-1}{2}} p (\text{mod } 3)$

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. $1^{\phi(12)} = 1 (\text{mod } 12)$ 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.

$5^{\phi(12)} = 5^4 = 625 = 52 \cdot 12 + 1 \equiv 1 (\text{mod } 12)$
$7^{\phi(12)} = 7^4 = 2401 = 200 \cdot 12 + 1 \equiv 1 (\text{mod } 12)$
$11^{\phi(12)} = 7^4 = 14641 = 1220 \cdot 12 + 1 \equiv 1 (\text{mod } 12)$.

$\phi(12) = 4$ together with $r^{\phi(12)} \equiv 1 (\text{mod } 12) \iff \gcd(r, 12) = 1$ 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 $11 = 12 - 1 \equiv -1 (\text{mod } 12)$ and $7 = 12 - 5 \equiv -5 (\text{mod } 12)$

So p is congruent to ± 1 or ± 5 modulo 12.

$p \equiv 1 (\text{mod } 12) \implies p = 12 \cdot m + 1$

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

$p \equiv -1 (\text{mod } 12) \implies p = 12 \cdot m - 1$

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

$p \equiv 5 (\text{mod } 12) \implies p = 12 \cdot m + 5$

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

$p \equiv -5 (\text{mod } 12) \implies p = 12 \cdot m - 5$

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

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

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

■

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

Pf.

$\phi(n) = 6$ 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. $n = p_0^{m_0} p_1^{m_1} ... p_k^{m_k}$ where p_i is prime, and $m_i \geq 0$, and k finite.

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

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

So, let's consider up to rearrangement

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

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 $p_i^{m_i-1} = 2]$)

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

$p_i - 1 = 1$ and $p_i^{m_i-1} = 2 \implies p_i = 2$ 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.

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

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

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.

So, $\phi(l) = q_0^0(q_0 - 1)...q_a^0(q_a - 1) = (q_0 - 1)...(q_a - 1) = 1$

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

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

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

Since 3 is prime, there's only one p_j in the product
and ($[m_j - 1 = 0$ and $p_j - 1 = 3]$ or $[p_j - 1 = 1$ and $p_j^{m_j-1} = 3]$)

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

$p_j - 1 = 1$ and $p_j^{m_j-1} = 3 \implies p_j = 2 \implies 2^{m_j-1} = 3$ 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,

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

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

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

So, $\phi(18) = 6$

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

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

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

The squares. Because:

```
def divisors (x):
    return [y for y in range(2, x) if x%y == 0 ]

[x for x in range(1,10000) if not(len(divisors(x))%2 == 0) and
len(divisors(x)) >= 1]

=> [4,9,16,25,36,49,64,81,100,121,144,169,196,225,256,289,324,361,
    400,441,484,529,576,625,676,729,784,841,900,961,1024,1089,1156,
    1225,1296,1369,1444,1521,1600,1681,1764,1849,1936,2025,2116,
    2209,2304,2401,2500,2601,2704,2809,2916,3025,3136,3249,3364,
    3481,3600,3721,3844,3969,4096,4225,4356,4489,4624,4761,4900,
    5041,5184,5329,5476,5625,5776,5929,6084,6241,6400,6561,6724,
    6889,7056,7225,7396,7569,7744,7921,8100,8281,8464,8649,8836,
    9025,9216,9409,9604,9801]
```

And $\tau(n) = \tau(p_1^{m_1} \cdots p_k^{m_k}) = (m_1 + 1) \cdots (m_k + 1)$ counts the number of divisors of n, where the prime decomposition of $n = p_1^{m_1} \cdots p_k^{m_k}$.

Suppose all the powers are even, then all the factors of the evaluation of τ at n are odd—i.e. $(m_i + 1) = (2k_i + 1)$ for some $k1, ...k_k \in \mathbb{Z}$. So $\tau(n)$ is odd. So the number of divisors of n is odd if n is a square.

Suppose there is a power m_j, that is odd, there exist a factor in the evaluation of τ at n is even—i.e. $(m_j + 1) = (2l + 1 + 1) = (2l + 2) = 2(l + 1)$ for some $l \in \mathbb{Z}$. So $\tau(n)$ is even, because it has at least one even term. So, this proves the only numbers that have an odd number of divisors are squares.