Math 261 — Exercise sheet 4

http://staff.aub.edu.lb/~nm116/teaching/2017/math261/index.html

Version: October 10, 2018

Answers are due for Wednesday 10 October, 11AM.

The use of calculators is allowed.

Exercise 4.1: CRT (40 pts)

Find all $x \in \mathbb{Z}$ such that $x \equiv 10 \bmod 100$ and $x \equiv 18 \bmod 31$. Simplify your answer.

Solution 4.1:

We are going to use the method seen in class. The first step is to check that CRT applies, by checking that 100 and 31 are coprime. This is rather obvious since $100 = 2^2 5^2$ and 31 is prime, but the second step is to find u and v such that $100u + 31v = 1$, so let us use Euclid's algorithm:

$$100 = 3 \times 31 + 7, \quad 31 = 4 \times 7 + 3, \quad 7 = 2 \times 3 + 1,$$

so this confirms that $\gcd(100, 31) = 1$, and working backwards we find that $u = 9$, $v = -29$ satisfy $100u + 31v = 1$.

As a result, we see that $100u = 1 - 31v$ is 0 mod 100 and 1 mod 31, and that $31v = 1 - 100u$ is 1 mod 100 and 0 mod 31. As a result, $a = 10 \times 31v + 18 \times 100u = 7210$ is 10 mod 100 and 18 mod 31, so it is a solution to our problem. But by CRT, the solutions correspond to a single element of $\mathbb{Z}/(100 \times 31)\mathbb{Z}$, i.e. are all congruent to each other mod 3100, so the solutions are the x such that $x \equiv 7210 \bmod 3100$. Since the question also asks to simplify our answer, our final answer is that the solutions are the x such that

$$x \equiv 1010 \bmod 3100.$$

Exercise 4.2: Eulers (10 pts)

Compute $\phi(261)$ and $\phi(600)$.

Solution 4.2:

Thanks to the (complete) factorizations $261 = 3^2 \times 29$ and $600 = 2^3 \times 3 \times 5^2$ and to the formula

$$\phi(n) = N \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right),$$

we find that

$$\phi(261) = 261(1 - 1/3)(1 - 1/29) = 3^2 \times 29 \times \frac{2}{3} \times \frac{28}{29} = 3 \times 2 \times 28 = 168$$

and that

$$\phi(600) = 2^3 \times 3 \times 5^2 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 2^2 \times 2 \times 5^1 \times 4 = 160.$$

Exercise 4.3: Inverse Euler (50 pts)

The goal of this exercise is to find all integers $n \in \mathbb{N}$ such that $\phi(n) = 4$.

1. (5 pts) Recall the value of $\phi(p^v)$ for $p, v \in \mathbb{N}$ and p prime.

2. (10 pts) Using the previous question, prove that if $p^v \mid n$, then $(p-1)p^{v-1} \mid \phi(n)$.

3. (20 pts) Using the previous question, prove that if $\phi(n) = 4$, then n cannot be divisible by a prime $p \geq 7$. Also prove that $3^2,\ 5^2 \nmid n$.

4. (15 pts) Find all n such that $\phi(n) = 4$.

   Hint: Think in terms of the factorisation of n. You should find that there are four such n — but you are required to prove this as part of this question!

Solution 4.3:

1. The non-invertibles in $\mathbb{Z}/p^v\mathbb{Z}$ are the elements represented by multiples of p. They thus represent a proportion $1/p$ of the p^v elements of $\mathbb{Z}/p^v$, so there are p^{v-1} of them. Thus $\phi(p^v) = p^v - p^{v-1} = (p-1)p^{v-1}$.

2. Let $p^{v'}$ be the exact power of p that divides n, so that $v' \geq v$ and we may write $n = p^{v'}m$ with $\gcd(p^{v'}, m) = 1$. Since ϕ is multiplicative, $\phi(n) = \phi(p^{v'})\phi(m)$ is divisible by $\phi(p^{v'}) = (p-1)p^{v'-1}$, whence also by $(p-1)p^{v-1}$ since $v'-1 \geq v-1$.

3. Let $p^v \mid n$, then by the previous question $(p-1)p^{v-1} \mid \phi(n) = 4$, so in particular $p - 1 \leq 4$, i.e. $p \leq 5$. Besides, if $v = 2$, then we get $(p-1)p \mid 4$, so $p \mid 4$, so $p = 2$. In other words, we cannot have $p^2 \mid n$ unless $p = 2$.

4. According to the previous question, the only possible prime factors of n are 2, 3, and 5, and 3 and 5 cannot be repeated factors. So we must have $n = 2^a 3^b 5^c$ for $a \geq 0$ and $b, c = 0$ or 1. Since $\phi$is multiplicative and since powers of distinct primes are coprime, we must then have $4 = \phi(n) = \phi(2^a)\phi(3^b)\phi(5^c)$. Now observe that

$$\phi(2^a) = \begin{cases} 1, & \text{if } a = 0, \\ 2^{a-1}, & \text{if } a \geq 1, \end{cases}$$

$$\phi(3^b) = \begin{cases} 1, & \text{if } b = 0, \\ 2, & \text{if } b = 1, \end{cases}$$

   and

$$\phi(5^c) = \begin{cases} 1, & \text{if } c = 0, \\ 4, & \text{if } c = 1. \end{cases}$$

   These observations clearly imply that the only combinations of (a, b, c) for which $\phi(n) = 4$ correspond to $n = 2^3$, $2^2 3$, 5, or $2 \cdot 5$.

   In conclusion, we have exactly four solutions: $n = 5$ or 8 or 10 or 12.

The exercise below is not mandatory. It is not worth any points, and is given here for you to practice. The solutions will be made available with the solutions to the other exercises.

Exercise 4.4: More inverse Eulers (0 pts)

This exercise is difficult, but doable. The questions are independent from each other.

1. Using the fact that $2018 = 2 \times 1009$ and that 1009 is prime, prove that there is no $n \in \mathbb{N}$ such that $\phi(n) = 2018$.

   Hint: Suppose 1009 *is a factor of* $\phi(n)$*. Where can this factor come from?*

2. Prove that for all $m \in \mathbb{N}$, there are at most finitely many[1] $n \in \mathbb{N}$ such that $\phi(n) = m$.

   Hint: Try to bound the prime factors of n *in terms of* m*.*

3. Prove that $\phi(n)$ is even for all $n \geq 3$.

   Hint: Start with the case when n *is a prime power.*

Solution 4.4:

1. Suppose n is such that $\phi(n) = 2018 = 2 \cdot 1009$. Factoring $n = \prod p_i^{v_i}$ with the p_i distinct primes and the $v_i \geq 1$, we get that

   $$1009 \mid 2018 = \phi(n) = \prod \phi(p_i^{v_i})$$

   since ϕ is multiplicative. Since 1009 is prime, Euclid's lemma tells us that 1009 must divide one of the factors $\phi(p_i^{v_i}) = (p_i - 1)p_i^{v_i - 1}$, and then another use of Euclid gives us $1009 \mid (p_i - 1)$ or $1009 \mid p_i^{v_i - 1}$. We are now going to prove that neither of these can happen.

   Indeed, if $1009 \mid (p_i - 1)$, then $p_i \equiv 1 \bmod 1009$, so $p_i = 1 + 1009x$ for some integer $x \geq 0$. Actually, $1 + 1009x$ is not prime for $x = 0$ nor for $x = 1$, and not for $x = 2$ either since $1 + 1009 \cdot 2 = 2019$ si divisible by 3 (sum of digits). So we must have[2] $x \geq 3$. But then $p_i > 3 \cdot 2018$, which is absurd since the fact that $(p_i - 1) \mid \phi(p_i^{v_i}) \mid \phi(n) = 2018$ implies that $p_i - 1 \leq 2018$.

   And if $1009 \mid p_i^{v_i - 1}$, then by unicity of factorisation we must have $p_i = 1009$ and $v_i = 2$; but this is absurd since in this case $\phi(p_i^{v_i}) = (p_i - 1)p_i = 1008 \cdot 1009$ is clearly way too large to divide $\phi(n) = 2018$.

   So we have reached a contradiction, which means that no such n exists.

2. Fix m, and let n be such that $\phi(n) = m$. Let p be a prime factor of n, and let $v = v_p(n)$ be the corresponding exponent, so that $n = p^v q$ with $q \in \mathbb{N}$ coprime to p. Then $m = \phi(n) = \phi(p^v)\phi(q)$ is divisible by $\phi(p^v) = (p - 1)p^{v-1}$, so $(p - 1)p^{v-1} \leq m$. This forces $p - 1 \leq m$, i.e. $p \leq m + 1$. and also shows that v cannot be arbitrarily large.

   So n has finitely many possible prime factors (the primes $\leq m+1$), and for each such prime p, $v_p(n)$ is bounded. So n has finitely many possible factorisations, i.e. there are finitely many candidates for such n.

[1] This means either finitely many or none.

[2] Actually, a computer search shows that the smallest x such that $1 + 1009x$ is prime is $x = 10$.

Remark: This is enough to prove that there are at most finitely many n such that $\phi(n) = m$, but of course, we have been rather sloppy, and as result we have probably grossly overestimated the number of such n. Estimating this number precisely would be much more complicated, cf. the previous exercise for instance!

3. Since $n \geq 3$, $n \neq 1$, so n has at least one prime factor p. Write again $n = p^v q$, where $v = v_p(n)$ so that $\gcd(p, q) = 1$. Then $(p-1)p^{v-1} = \phi(p^v) \mid \phi(n)$.

   Now clearly $p-1$ is even, except if $p = 2$. So we are done if we can take $p \neq 2$. In other words, the only case for whcih we have not yet proved that $\phi(n0$ is even is the case where $n = 2^v$ is a power of 2. But since $n \geq 3$, we have $v \geq 2$, so $\phi(n) = \phi(2^v) = 2^{v-1}$ is again even as $v - 1 > 0$.