Math 261 — Exam 1

October 15, 2018

The use of notes and books is **NOT** allowed.

Exercise 1: Since today is October 15th... (30 pts)

In this exercise, you must justify the primality of any number larger than 50.

1. (8 pts) Find the factorization of 1510 into primes. Deduce the **number** of positive divisors of 1510.
2. (8 pts) Find the factorization of 1015 into primes. Deduce the **sum** of the postive divisors of 1015.
3. (14 pts) Compute $\phi(l)$, where $l = \operatorname{lcm}(1510, 1015)$.

Solution 1:

1. Clearly $1510 = 10 \cdot 151 = 2 \cdot 5 \cdot 151$. If 151 were composite, it would have at least one factor $\leq \sqrt{151} < 13$. But 151 is not divisible by 2 (last digit) nor by 3 (sum of digits) nor 5 (last digit) nor 7 (else $7 \mid (151 - 140) = 11$, absurd) nor 11 (alternate sum of digits), so it is prime and the complete factorisation is $2 \cdot 5 \cdot 151$. So the number of divisors is $(1+1)(1+1)(1+1) = 8$.
2. Clearly 1015 is divisible by 5, and in fact it is $5 \cdot 203$. The cofactor 203 is not divisible by 2 nor 3 nor 5, but we spot that $203 = 210 - 7 = 7 \cdot 30 - 7 = 7 \cdot 29$. Since 29 is prime, the complete factoriation is $1015 = 5 \cdot 7 \cdot 29$. Therefore, the sum of the divisors is $(1+5)(1+7)(1+29) = 1440$.
3. By comparing the factorisations, we see that the factorisation of l is $l = 2 \cdot 5 \cdot 7 \cdot 29 \cdot 151$. The multiplicativity of ϕ and the fact that $\phi(p) = p - 1$ for p prime then show that
$$\phi(l) = (2-1)(5-1)(7-1)(29-1)(151-1) = 100800.$$

Exercise 2: Quotient=remainder (10 pts)

Find all positive integers $n \in \mathbb{N}$ such that in the Euclidean division of n by 261, the quotient is the same as the remainder.

Solution 2:

The divisor of any n by 261 yields $n = 261q + r$ with $q, r \geq 0$ and $r < 261$. If we impose that $q = r$, we get that $n = 261r + r = 262r$ with $0 \leq r < 261$. Since we want $n > 0$, actually r cannot be 0.

Conversely, if $n = 262r$ with $0 < r < 262$, then we have $n = 261r + r$, which since $0 \leq r < 261$ is the division of n by 261 by unicity of the quotient and remainder.

Conclusion: these n are the multiples of 262 between 262 and $262 \cdot 260$ included.

Exercise 3: An lcm (10 points)

Let $n \in \mathbb{N}$. Determine $\operatorname{lcm}(n, n+1)$ in terms of n.

Solution 3:

We know that $\operatorname{lcm}(n, n+1) = n(n+1)/\gcd(n+1)$. But for $u = -1$ and $v = 1$ we have

$$nu + (n+1)v = 1$$

which by Bézout shows that $\gcd(n, n+1) = 1$. So $\operatorname{lcm}(n, n+1) = n(n+1)$ for all $n \in \mathbb{N}$.

Exercise 4: All in one (50 pts)

The purpose of the exercise is to find all integers $x, y \in \mathbb{Z}$ such that

$$\begin{cases} 21x + 30y = 6, \\ x \equiv 2 \pmod 7, \\ y \equiv 1 \pmod{10} \end{cases} \qquad (\star)$$

This exercise is designed so you can explain how to solve a question even if you were unable howto solve the previous one.

1. (12 pts) First of all, let us focus on the equation $21x + 30y = 6$. Explain why there are numbers e, f, g, h such that the solutions are given by $x = e + ft$, $y = g + ht$ for $t \in \mathbb{Z}$, and find these numbers.

In the next questions, we are going to determine which $t \in \mathbb{Z}$ ensure that the other equations $x \equiv 2 \pmod 7$ and $y \equiv 1 \pmod{10}$ are also satisfied.

2. (10 pts) We now plug in the condition $x \equiv 2 \pmod 7$, that is to say $e + ft \equiv 2 \pmod 7$ where e and f were found above. Explain why this is equivalent to $t \equiv k \pmod 7$, where k is a constant that you must determine.

3. (5 pts) Similarly, show that the condition $g + ht \equiv 1 \bmod 10$ (where g and h were found in part 1.) is equivalent to the condition $t \equiv l \bmod 10$, where l is a constant that you must determine.

4. (18 pts) Explain why the two conditions

$$\begin{cases} t \equiv k \pmod 7, \\ t \equiv l \pmod{10} \end{cases}$$

found in the previous two parts are equivalent to $t \equiv m \pmod{70}$ for some constant m, and find such an m.

5. (5 pts) Finally, what are the solutions to the system of equations $(\star)$?

Solution 4:

1. Clearly $\gcd(21, 30) = 3$. Since $3 \mid 6$, the equation has infinitely many solutions. To find them, we first simplify by 3, which yields

$$7x + 10y = 2,$$

then we look for a particular solution, either using Bézout (which gives us a solution for $7x+10y = 1$ and then we multiply everything by 2) or by spotting directly that $x = 6$, $y = -4$ is a solution. We then know that the solutions are exactly

$$x = 6 + 10t, \ y = -4 - 7t \quad (t \in \mathbb{Z}).$$

2. We now want $6 + 10t \equiv 2 \pmod 7$, i.e. $3t \equiv 3 \pmod 7$ as $10 \equiv 3$ and $2 - 6 \equiv 3 \pmod 7$. Since 3 is invertible mod 7 (because coprime with 7), this is equivalent to $t \equiv 3^{-1}3 \pmod 7$, where 3^{-1} means the inverse of 3 mod 7. We could compute this inverse and then multiply it by 3, but of course the result is going to be 1 so we don't need to bother finding the inverse! So the condition is $t \equiv 1 \pmod 7$.

3. This time we want $-4 - 7t \equiv 1 \pmod{10}$, whence $3t \equiv 5 \pmod{10}$. Again 3 is invertible mod 10 so this is equivalent to $t \equiv 3^{-1}5 \pmod{10}$ where this time 3^{-1} denotes the inverse of 3 mod 10. To compute $3^{-1}5$, there are (at least) three ways:

   - Compute 3^{-1}, which turns out to be $7 = -3$ (either by Bézout or by inspection), and multiply by 5: we find $t \equiv 5 \pmod{10}$.
   - We have just seen that $-4 - 7t \equiv 1$ if and only if $t \equiv l$ for some constant l that is unique mod 10, so we can try all values of l until we find the one that works. We see that for $t = 5$, $-4 - 7t = -49 \equiv 1 \pmod{10}$, so l must be 5 mod 10.
   - We can use Chinese remainders! As 2 and 5 are coprime, $\mathbb{Z}/10\mathbb{Z}$ is the same as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Under this correspondence, $3^{-1}5$ becomes $(3^{-1}5, 3^{-1}5) = (1^{-1}1, 0) = (1, 0)$ where the first coordinate is mod 2 and the second is mod 5. So we are looking for an odd multiple of 5, which is of course 5 (we know it's unique mod 10).

4. This is Chinese remainders, which apply here because 7 and 10 are coprime. To find m, wecould try the values of m one by one until we stumble upon the unique solution. Instead, let us find a Bézout relation between 7 and 10, for instance

$$7 \times 3 + 10 \times -2 = 1$$

(actually we have already done this for question 1.). So we know that m is given by $k \cdot 10 \times -2 + l \cdot 7 \times 3$, whence $m = -20 + 105 = 85 \equiv 15 \pmod{70}$. So the condition is $t \equiv 15 \pmod{70}$.

5. The fact that $t \equiv 15 \pmod{70}$ translates into $t = 15 + 70s$, $s \in \mathbb{Z}$. Plugging this into $x = 6 + 10t$, $y = -4 - 7t$, we get that the solutions of $(\star)$ are

$$x = 156 + 700s, \ y = -109 - 490s \quad (s \in \mathbb{Z}).$$

END