Math 261 — Exam 1

October 4, 2017

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

Exercise 1: Since today is October 4th... (10 pts)

1. (4 pts) Compute the factorization of 104 into primes.
2. (6 pts) Deduce the number of divisors of 104, the sum of these divisors, and the value of $\phi(104)$.

Solution 1:

1. Clearly, 104 is even, so we divide it by 2. We get $104 = 2 \times 52$, and 52 is again even, so we keep going... we finally get $104 = 2^3 \times 13$. Now, 13 is prime (if it were not, it would be divisible by a prime $\leqslant \sqrt{13} < 4$, so by 2 or 3, but it isn't), so this is the complete factorization of 104:

$$\boxed{104 = 2^3 \times 13.}$$

2. The number of divisors is thus

$$\sigma_0(104) = (1+3)(1+1) = \boxed{8},$$

the sum of these divisors is

$$\sigma_1(104) = (1+2+4+8)(1+13) = 15 \times 14 = \boxed{210},$$

and finally

$$\phi(104) = 104(1-1/2)(1-1/13) = 104\frac{1}{2}\frac{12}{13} = \frac{104}{13}6 = 8 \times 6 = \boxed{48}.$$

Exercise 2: Consecutive composites (16 pts)

1. (4 pts) Find 5 consecutive composite (i.e. not prime) integers $\leqslant 100$.
2. (12 pts) Find 2017 consecutive composite integers.

   Hint: consider numbers of the form $n! + m$, where $n, m \in \mathbb{N}$, $m \leqslant n$, and $n! = 1 \times 2 \times 3 \times \cdots \times n$.

Solution 2:

1. The smallest solution is $\boxed{24, 25, 26, 27, 28}$. This is not the only one; for instance, 32, 33, 34, 35, 36 also works.

2. (12 pts) If $m \leqslant n$, then m divides $n! = 1 \times 2 \times 3 \times \cdots \times m \times \cdots \times n$, so $m \mid (n! + m)$. Since $n! + m > m$, if $m \neq 1$ this implies that $n! + m$ is composite. So the integers

$$n! + 2, n! + 3, \cdots, n! + n$$

are all composite, and of course they are consecutive. Since this sequence contains $n - 1$ integers, and we want a sequence of length 2017, we take $n = 2018$, and get

$$\boxed{2018! + 2,\ 2018! + 3,\ \cdots,\ 2018! + 2018.}$$

Remark: These integers have 5795 digits each!

Exercise 3: Making change (11 pts)

1. (8 pts) Find all integers $x, y \in \mathbb{Z}$ such that $20x + 50y = 10000$.

2. (3 pts) Deduce how many different ways there are to pay \$10000 using only banknotes of \$20 and \$50.

Solution 3:

1. Since $\gcd(20, 50) = 10$ divides 10000, there are solutions, and the equation can be simplified into

$$2x + 5y = 1000.$$

One solution is $x = 500$, $y = 0$, so the solutions are given by

$$\boxed{x = 500 - 5t,\ y = 2t,\ t \in \mathbb{Z}.}$$

2. This corresponds to finding the solutions of the above equation with $x \geqslant 0$ and $y \geqslant 0$. In other words, we need $500 - 5t \geqslant 0$, so $t \leqslant 100$, and $2t \geqslant 0$, so $t \geqslant 0$. So the solutions with $x \geqslant 0$ and $y \geqslant 0$ are given by the $t \in \mathbb{Z}$ such that $0 \leqslant t \leqslant 100$. There are thus $\boxed{101}$ ways.

Exercise 4: Only 2 (20 pts)

Find all $n \in \mathbb{N}$ such that $\phi(n) = 2$.

Solution 4:

Clearly $n = 1$ does not work, so we can consider a prime divisor p of n. We can write $n = p^v m$, where $v = v_p(n) \in \mathbb{N}$ and m is coprime to p^v; then, since ϕ is multiplicative, we have

$$2 = \phi(n) = \phi(p^v)\phi(m) \geqslant \phi(p^v) = (p-1)p^{v-1} \geqslant p - 1,$$

so necessarily $p \leqslant 3$. Thus the only possible prime divisors of n are 2 and 3.

If $n = 2^a$, then as $\phi(n) = 2^{a-1}$ we must have $a = 2$, so $n = 4$.

If $n = 3^b$, then as $\phi(n) = 2 \cdot 3^{b-1}$ we must have $b = 1$, so $n = 3$.

Finally, if $n = 2^a 3^b$ with $a, b \neq 0$, then

$$\phi(n) = \phi(2^a)\phi(3^b) = 2^{a-1} \times 2 \cdot 3^{b-1}$$

so we must have $a = b = 1$, whence $n = 6$.

Conclusion: $\phi(n) = 2$ exactly when $n = \boxed{3 \text{ or } 4 \text{ or } 6.}$

Exercise 5: A system of congruences (15 pts)

Find all $x \in \mathbb{Z}$ satisfying both

$$\begin{cases} 4x \equiv 5 \pmod 7 \\ 5x \equiv 3 \pmod 8 \end{cases}$$

Solution 5:

We are going to solve these equations independently, and then apply Chinese remainders.

Since 4 is coprime to 7, it is invertible mod 7; its inverse is 2. So the first equation is equivalent to $x \equiv 2 \times 5 \equiv 3 \pmod 7$.

Since 5 is coprime to 8, it is invertible mod 8; its inverse is 5. So the second equation is equivalent to $x \equiv 5 \times 3 \equiv -1 \pmod 8$.

Now, since 7 and 8 are coprime, we can apply Chinese remainders to find all $x \in \mathbb{Z}/56\mathbb{Z}$ such that $x \equiv 3 \pmod 7$ and $x \equiv -1 \pmod 8$. We know that the solution will exist and be unique in $x \in \mathbb{Z}/56\mathbb{Z}$.

In order to find this unique solution, we first look for u and v such that $7u + 8v = 1$, we see that $u = -1$, $v = 1$ works. So we get that

$$-7 \equiv 0 \pmod 7, \quad -7 \equiv 1 \pmod 8$$

and that

$$8 \equiv 1 \pmod 7, \quad 8 \equiv 0 \pmod 8.$$

We thus find the x such that

$$x \equiv 3 \pmod 7, \quad x \equiv -1 \pmod 8$$

as

$$x = 3 \times 8 + -1 \times -7 = 31.$$

(At this point, it is a good idea to check our computations by verifying that 31 is indeed a solution to both original equations.)

So the original equations are equivalent to $x \equiv 31 \pmod{56}$. In other words, the solutions are the

$$\boxed{x = 31 + 56t,\ t \in \mathbb{Z}.}$$

Exercise 6: Irreducible polynomials over $\mathbb{Z}/2\mathbb{Z}$ (28 pts)

1. (6 pts) Find all irreducible polynomials of degree 2 over $\mathbb{Z}/2\mathbb{Z}$.
2. (12 pts) Use the previous question and a Euclidian division to deduce that the polynomial $x^4 + x + 1$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$.
3. (10 pts) Find all irreducible polynomials of degree 3 over $\mathbb{Z}/2\mathbb{Z}$.

Solution 6:

1. A polynomial of degree 2 is irreducible if and only if it has no roots (this is a general fact and has nothing to with $\mathbb{Z}/2\mathbb{Z}$; this is just saying that a polynomial of degree 2 is either irreducible or factors as a product of two polynomials of degree 1).

   So let $ax^2 + bx + c$ be a polynomial of degree 2, with $a, b, c \in \mathbb{Z}/2\mathbb{Z}$. We need $a \neq 0$ (else it's not of degree 2), and since $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, we must have $a = 1$.

   We need our polynomial not to vanish at $x = 0$, so $c \neq 0$ so $c = 1$, and neither at $x = 1$, so $1 + b + 1 = b \neq 0$, so $b = 1$.

   We have thus proved that there is exactly one irreducible polynomial of degree 2:

   $$\boxed{x^2 + x + 1.}$$

2. Let $f(x) = x^4 + x + 1$. We have $f(0) = f(1) = 1 \neq 0$, so this polynomial has no roots; since it has degree 4, it is thus either irreducible, or a product of two irreducible polynomials of degree 2 (any other factorization pattern would include at least one factor of degree 1, which would yield a root).

   We saw in the previous question that there is only one irreducible polynomial of degree 2, namely $g(x) = x^2 + x + 1$. So let us see if $f(x)$ is divisible by $g(x)$, by performing the Euclidian division of f by g. We find quotient $= x^2 + x$ and remainder $= 1$. Since the remainder is not zero, g does not divide f. So f must be irreducible.

   Remark: There was another way to show that. Indeed, if f had been a product of two irreducibles of degree 2, then since these irreducibles could only be g, and we would necessarily have had

   $$f = g^2 = (x^2 + x + 1)^2 = x^4 + x^2 + 1.$$

   This is not the case, so f is irreducible.

3. The degrees of the irreducible factors of a polynomial of degree 3 can be either $1+1+1$, or $1+2$, or 3 (again, this has nothing to do with $\mathbb{Z}/2\mathbb{Z}$ in particular). So it is irreducible if and only if it has no root (just like in degree 2; however this is no longer true in degree 4 and higher).

So let $ax^3 + bx^2 + cx + d$ be of degree 3. We must have $a \neq 0$, whence $a = 1$. Next, this polynomial will be irreducible if and only if it has no roots, that is to say if it does not vanish at $x = 0$ nor at $x = 1$. The first condition means that $d \neq 0$, so $d = 1$. The second condition means that $b + c \neq 0$, so $b + c = 1$, so either $b = 0$, $c = 1$, or $b = 1$, $c = 0$. We thus have two irreducibles of degree 3:

$$\boxed{x^3 + x + 1 \text{ and } x^3 + x^2 + 1.}$$

END