Fall 2021 – Math 328K – 55385

Final exam

Thursday, December 9, 9:00

- Write your name clearly readable on the top of **every page** you write!
- Prove every statement you write.
- You can use all theorems from the lectures and homeworks without giving a proof.
- Do not use a red pen.
- No phones, calculators, books, notes, etc. are permitted.
- Good luck!

Problem 1. Choose all right answers (could be none, one or more than one).

a) Which of the following statements are true for every ring R? (0 and 1 are the neutral elements for addition and multiplication in R)

☐ $xy = yx$ for all $x, y \in R$.

☐ For all $x \in R$, there exists $k \in \mathbb{N}$ such that $x^k = 1$.

☒ $R^\times \neq \varnothing$.

☐ If $x, y, z \in R$, $x \neq 0$, and $xy = xz$, then $y = z$.

☒ If $n \in \mathbb{N}$, $x \in R$, and $1 - x^2 \in R^\times$, then $\sum_{k=0}^{n-1} x^{2k} = (1 - x^2)^{-1}(1 - x^{2n})$.

b) What is the value of the continued fraction $[6, 3, 6, 3, 6, 3, 6, 3, 6, 3, 6, \dots]$?

☐ $\sqrt{10}$

☐ π

☐ $\sqrt{7}/2$

☒ $\sqrt{11} + 3$

☐ $(\sqrt{5} + 1)/2$

c) Which of the following statements are true?

☒ There is a primitive root in $\mathbb{Z}/4\mathbb{Z}$.

☐ If $x \in \mathbb{Z}/p\mathbb{Z}$, p prime, then a power of x is a primitive root.

☐ If $x \in \mathbb{Z}/p\mathbb{Z}$, p prime, then x is a power of a primitive root.

☒ If p is prime and $d \mid p - 1$, then $\mathbb{Z}/p\mathbb{Z}$ has an element of order d.

☐ If p is prime and $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, there exists $b \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $a = b^5$.

d) Bob sent the encrypted message LXYARVN, which he had encrypted using a Caesar cipher. What could the plaintext be?

☐ DIVISOR

☐ QUOTIENT

☐ INTEGER

☒ COPRIME

☐ EXPONENTIATION

Problem 2. Let $x, y \in \mathbb{Z}$ be coprime. Show that $(x+2y, y+2x)$ is either 1 or 3.

Solution 2. Recall that $(a, b) = (a + bc, b)$ for all $a, b, c \in \mathbb{Z}$. Therefore

$$(x+2y, y+2x) = (x+2y-2(y+2x), y+2x) = (-3x, y+2x) = (3x, y+2x-3x) = (3x, y-x).$$

Now assume p is a common prime divisor of $3x$ and $y - x$. Then either $p \mid 3$ or $p \mid x$. In the latter case p also divides $y = x + (y - x)$, contradicting the assumption that $(x, y) = 1$. So $p \mid 3$ or, equivalently, $p = 3$. Hence we know that the only prime which can be a common divisor of $3x$ and $y - x$ is 3.

So $(3x, y - x) = 3^k$ for some k. If $k \geq 2$, then $9 \mid 3x$, so $3 \mid x$. By the same argument as before this implies $3 \mid y$ and leads to a contradiction. Consequently, $(x + 2y, y + 2x)$ can only be 1 or 3.

Problem 3.

a) Which integers up to 100 have exactly 10 positive divisors (including 1 and itself)?

b) Are there integers up 100 with more than 10 positive divisors?

Solution 3.

a) Let τ be the number of divisors function, as defined in class. It is multiplicative, so if $n = p_1^{i_1} \dots p_k^{i_k}$ for distinct primes p_j and exponents $i_j \geq 1$, then

$$\tau(n) = (i_1 + 1) \cdots (i_k + 1).$$

There are only two possibilities to get $\tau(n) = 10 = 2 \cdot 5$: either $n = p^9$ for some prime p, or $n = pq^4$ for two different primes p and q. The first option does not occur for $n \leq 100$ since $2^9 = 512$. In the second case, if $q \geq 3$ then $pq^4 \geq 2 \cdot 3^4 = 162 > 100$. So $q = 2$, i.e. $n = 16p$ for some odd prime p, which has to be 3 or 5. So the only two numbers under 100 with exactly 10 divisors are 48 and 80.

b) No integer up to 100 has 11 divisors (1024 is the lowest number with 11 divisors). However some numbers have 12 divisors: similarly to the above, the decompositions $12 = 6 \cdot 2 = 4 \cdot 3 = 3 \cdot 2 \cdot 2$ suggest integers of the form p^{11}, $p^5 q$, $p^3 q^2$ or $p^2 qr$ for pairwise different primes p, q, r. The numbers of this form below 100 are:

$$2^5 \cdot 3 = 96, \quad 2^3 \cdot 3^2 = 72, \quad 2^2 \cdot 3 \cdot 5 = 60, \quad 2^2 \cdot 3 \cdot 7 = 84, \quad 3^2 \cdot 2 \cdot 5 = 90.$$

Of course, to solve the problem it was enough to find one example.

Problem 4. A natural number $n \in \mathbb{N}$ is called *perfect* if it is equal to the sum of its positive divisors except itself, or equivalently if $\sigma(n) = 2n$. *(Recall that $\sigma(n)$ is the sum of positive divisors of n including n, a multiplicative function.)*

Show for $k \in \mathbb{N}$ that the number

$$n = 2^{k-1}(2^k - 1)$$

is perfect if and only if $2^k - 1$ is prime.

.

Solution 4. Since σ is a multiplicative function and $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$ we can compute

$$\sigma(n) = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)\sigma(2^k - 1).$$

So $\sigma(n) = 2n$ is equivalent to the equation

$$(2^k - 1)\sigma(2^k - 1) = 2^k(2^k - 1) \quad \Leftrightarrow \quad \sigma(2^k - 1) = 2^k,$$

that is the equation $\sigma(p) = p + 1$, if we write $p = 2^k - 1$. Of course p and 1 are always divisors of p, so $\sigma(p) = p + 1$ if and only if there are no other divisors, that is if p is prime. This shows that n is perfect if and only if p is prime.

Problem 5. Let $n = p_1 \cdots p_k$ be a product of distinct odd primes and let $x \in \mathbb{Z}/n\mathbb{Z}$. Show that

$$x^{\phi(n)+1} = x.$$

Solution 5. For each $i \in \{1, \ldots, k\}$ we have $\phi(p_i) \mid \phi(n)$. Say $\phi(n) = \phi(p_i)d_i$ for some $d_i \in \mathbb{Z}_+$. Then

$$x^{\phi(n)+1} \bmod p_i = x \cdot (x^{\phi(p_i)})^{d_i} \bmod p_i = (x \bmod p_i) \cdot ((x \bmod p_i)^{\phi(p_i)})^{d_i}.$$

If $x \bmod p_i \in (\mathbb{Z}/p_i\mathbb{Z})^\times$ then this equals $x \bmod p_i$ by Euler's theorem. On the other hand, if $x \bmod p_i \notin (\mathbb{Z}/p_i\mathbb{Z})^\times$, then $x \bmod p_i = 0 \bmod p_i$, and we still have $x^{\phi(n)+1} \bmod p_i = x \bmod p_i$.

We showed that $(x^{\phi(n)+1} - x) \bmod p_i = 0 \bmod p_i$ for each i. By the Chinese Remainder Theorem, this implies that $x^{\phi(n)+1} - x = 0 \bmod n$, that is $x^{\phi(n)+1} = x$.

Problem 6. Consider the equation

$$x^4 + 2x + 5 = 0.$$

How many different solutions does it have in $\mathbb{Z}/500\mathbb{Z}$? (you don't need to find the solutions, just their number!)

Here is a table of the squares, cubes, and fourth powers of 1–digit numbers:

x	0	1	2	3	4	5	6	7	8	9
x^2	0	1	4	9	16	25	36	49	64	81
x^3	0	1	8	27	64	125	216	343	512	729
x^4	0	1	16	81	256	625	1296	2401	4096	6565

Solution 6. Let $f(x) = x^4 + 2x + 5$. We compute

$$\begin{aligned} f(0) &= 5 \\ f(1) &= 8 \\ f(2) &= 25 \\ f(3) &= 92 \\ f(4) &= 269 \end{aligned}$$

So there are two solutions in $\mathbb{Z}/5\mathbb{Z}$, namely $[0]$ and $[2]$. Since $[f'(0)]_5 = [2]_5$ and $[f'(2)]_5 = [34]_5$ Hensel's Lemma shows that there is a unique lift of each of these solutions to $\mathbb{Z}/25\mathbb{Z}$, and also to $\mathbb{Z}/125\mathbb{Z}$.

On the other hand, there two solutions in $\mathbb{Z}/4\mathbb{Z}$, $[1]$ and $[3]$. Since $500 = 4 \cdot 125$ the Chinese Remainder Theorem tells us that the equation has $2 \cdot 2 = 4$ solutions in $\mathbb{Z}/500\mathbb{Z}$.

Problem 7. Let $a, m \in \mathbb{Z}_+$, $a > 1$, and let $x = [a]_m \in \mathbb{Z}/m\mathbb{Z}$.

a) Assuming that $m = a^n - 1$ for some $n \in \mathbb{N}$, show that $\operatorname{ord}(x) = n$.

b) Assuming that $m = a^n + 1$ for some $n \in \mathbb{N}$, show that $\operatorname{ord}(x) = 2n$.

Solution 7.

a) Let $k = \operatorname{ord}(x)$. First, $x^n = [a^n]_m = [m+1]_m = [1]_m$, so $k \leq n$. Next, $[a^k]_m = [1]_m$, so $m \mid a^k - 1$. In particular $a^n - 1 = m \leq a^k - 1$. Since $a > 1$ this implies $n \leq k$.

b) Again let $k = \operatorname{ord}(x)$. Now $x^n = [a^n]_m = [m-1]_m = [-1]_m$. Then $x^{2n} = [-1]_m^2 = [1]_m$, so $k \mid 2n$. As before $[a^k]_m = [1]_m$, so $m \mid a^k - 1$. In particular $a^n \leq a^n + 1 = m \leq a^k - 1 \leq a^k$. This implies $k \geq n$. Together with $k \mid 2n$ we know that k is either n or $2n$. If $k = n$ then $[-1]_m = x^n = [1]_m$, which is only possible if $m = 2$. This would contradict the assumption $a > 1$. So $k = 2n$.