Math 4400 Midterm 2

July 21, 2017

Name: Solutions

You may assume, without proof:

- If $a, b \in \mathbb{N}$ and $ab = 1$, then $a = 1$ and $b = 1$
- If $a \mid b$ and $b \mid c$, then $a \mid c$
- If $ac \mid bc$ and $c \neq 0$, then $a \mid b$.

Question	Points	Score
1	10	
2	15	
3	10	
4	20	
5	15	
6	20	
7	10	
Total:	100	

1. (a) (5 points) Compute the order of [22] in $\mathbb{Z}/99\mathbb{Z}$.

$$o(22) = \frac{99}{\gcd(99,22)} = \frac{99}{11} = 9$$

$99 = 3^2 \cdot 11$,

$22 = 2 \cdot 11$, so $\gcd = 11$.

(b) (5 points) Compute the order of [21] in $\mathbb{Z}/99\mathbb{Z}$.

$21 = 7 \cdot 3$, $99 = 3^2 \cdot 11$ $\Rightarrow \gcd = 3$

$$o(21) = \frac{99}{3} = 33$$

2. (15 points) Solve the congruence, $x^{17} \equiv 18 \mod 77$ (no need to simplify your answer mod 77)

$77 = 7 \cdot 11 \Rightarrow \varphi(77) = 6 \cdot 10 = 60.$

Check: $\gcd(17, 60) = 1,$

$\gcd(18, 77) = 1$

Thus, $x = 18^u$, where $17u \equiv 1 \mod 60.$

$u = ?$ Euclidean algo:

$60 = 3 \cdot 17 + 9, \quad 17 = 1 \cdot 9 + 8, \quad 9 = 1 \cdot 8 + 1$

$\Rightarrow 9 - 8 = 1 \Rightarrow 2 \cdot 9 - 17 = 1,$

$\Rightarrow 2 \cdot 60 - 7 \cdot 17 = 1 \Rightarrow x \equiv 18^{-7} \equiv 18^{53} \mod 77$

3. (10 points) Let $R = \mathbb{Z}[\sqrt{7}]/11\mathbb{Z}[\sqrt{7}]$. Compute the inverse of $3 + 2\sqrt{7}$ in R.

$N(3+2\sqrt{7}) = 9-4.7 = -19 \equiv 3$

3^{-1} mod 11? Easy enough to do by brute force: $3 \cdot 4 = 12 \equiv 1$ mod 11.

$\Rightarrow (3+2\sqrt{7}) = (3-2\sqrt{7}) \cdot 4 \equiv 12 - 8\sqrt{7}$

$\equiv 1 + 3\sqrt{7}$

4. (20 points) True or false: print a T or an F on each line! Let G be a finite group and let k be a field. Also, 163 and 89 are indeed prime numbers.

(a) ___ Any subgroup of a non-abelian group is non-abelian

(b) ___ Any subgroup of an abelian group is abelian

(c) ___ [3] is a zero-divisor in $\mathbb{Z}/6\mathbb{Z}$

(d) ___ It's possible for a primitive 10^{th} root of unity in k to be a 5^{th} root of unity in k.

(e) ___ It's possible for a 10^{th} root of unity in k to be a primitive 5^{th} root of unity in k.

(f) ___ $\mathbb{Z}/9\mathbb{Z}$ is a field under the usual addition and multiplication operations.

(g) ___ It's possible for a group of order 10 to have a subgroup of order 3

(h) ___ It's possible for a group of order 10 to have a subgroup of order 5

(i) ___ -1 is a square modulo 163

(j) ___ 2 is a square modulo 89

5. (15 points) Let G be a group, and let $g \in G$ be an element of order n. Prove that the elements $g, g^2, g^3, \ldots, g^n$ are all distinct.

Suppose $g^i = g^j$ for some $1 \le i < j \le n$.

Then $e = g^{j-i}$. But

$0 < j-i \le n-i < n$ (in particular, $0 < j-i < n$)

This contradicts the assumption that $o(g) = n$ (contradicts the minimality of n)

6. (20 points) Prove that there are infinitely many primes congruent to 3 modulo 4. (Hint: suppose there are only finitely many such primes and let $S = \{p_1, \ldots, p_n\}$ of all primes congruent to 3 modulo 4, except for 3 itself. Prove that $4p_1p_2\cdots p_n + 3$ is divisible by a prime that's congruent to 3 modulo 4 to get a contradiction.)

By uniqueness (and existence) of factorization, $\exists$ primes, $q_1, \ldots, q_r$ s.t. $m = q_1 q_2 \cdot \ldots \cdot q_r$. Note: m is odd, so $q_i \neq 2$ for all i. Thus $q_i \equiv 1 \bmod 4$ or $q_i \equiv 3 \bmod 4$.

If $q_i \equiv 1 \bmod 4$ for all i, then $m \equiv q_1 \cdots q_r \equiv 1 \cdot 1 \cdot \ldots \cdot 1 \equiv 1 \bmod 4$. But $4 \mid m-3$, so $m \equiv 3 \bmod 4$. Thus $\exists i$ s.t. $q_i \equiv 3 \bmod 4$. Also, $\forall p \in S$, $p \nmid m$; otherwise $p \mid (m - 4p_1 \cdots p_n)$. But $p \nmid 3$.

$\Rightarrow q_i \notin S$; note that $3 \nmid m$, since otherwise $3 \mid m-3 = 4p_1 \cdots p_n$, but this violates uniqueness of factorization.

Contradiction!

7. (10 points) Let p be an odd prime number and suppose that a is a square mod p. Prove that a is not a primitive root mod p (i.e. a is not a primitive $(p-1)^{th}$ root of unity in $\mathbb{Z}/p\mathbb{Z}$.)

If $a \equiv 0 \mod p$, then certainly a is not a root of unity. So assume $a \not\equiv 0 \mod p$. Let $a \equiv b^2 \mod p$.

$$\Rightarrow a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \underset{\substack{\uparrow \\ \text{Fermat's Little Thm}}}{\equiv} 1$$

$\Rightarrow$ a is not primitive.

(note: $\frac{p-1}{2} \in \mathbb{Z}$, since p is odd)