Peter Cholak and Juan Migliore Math 222 - Exam 1 Wednesday, February 28

Except where noted, be sure to show all your work.

(4 points each for a total of 20 points) **Define** the following terms:
a) $\sqrt[n]{z}$ over the complex numbers.

$\sqrt[n]{z}$ over the complex numbers is the set of all the complex numbers x with $x^n = z$.

b) A *primitive* complex nth root of unity.

A complex root of unity whose order is n.

c) m and n are *relatively prime.*

The integers m and n are *relatively prime* if their greatest common divisor is 1.

d) The *multiplicative inverse* of a nonzero number a in $\mathbb{Z}_p$ (p a prime).

The *multiplicative inverse* of a nonzero number a in $\mathbb{Z}_p$ is the number b in $\mathbb{Z}_p$ with $ab \equiv ba \equiv 1$ modulo p.

e) An equation $a_0x^n + a_1x^{n-1} + \dots a_{n-1}x + a_n = 0$ is *solvable by radicals* (or *algebraically resolvable*) if ...

each of its root has an algebraic expression in the coefficients $\{a_0, a_1, \dots, a_n\}$.
(2 points each for a total of 10 points) Answer **True** or **False** - no work required:
a) the possible orders of elements in $\mathbb{Z}_{19}$ are 1 and 19.

Answer: False. The possible orders of elements in $\mathbb{Z}_{17}$ are all the positive divisors of $18 = 19 - 1$. They are just $1, 2, 3, 6, 9, 18$.

b) 4 is the multiplicative inverse of 3 in $\mathbb{Z}_{11}$.

Answer: True. $4 \times 3 = 12 \equiv_{11} 1$.

c) The coefficient of a^6b^8 in $(a^2 - 2b)^{11}$ is divisible by 11.

Answer: True. The coefficient of a^6b^8 in $(a^2 - 2b)^{11}$ is $\binom{11}{3}(-2)^8 = \frac{11!}{(3!)(8!)}(-2)^8$, which is divisible by 11.

d) 3 has a multiplicative inverse in $\mathbb{Z}_{18}$.

Answer: False. The gcd of 3 and 18 is 3. Since 3 and 18 are not relatively prime, 3 does not have a multiplicative inverse in $\mathbb{Z}_{18}$.

e) 3 is an primitive element of $\mathbb{Z}_{13}$.

Answer: False. The order of 3 is 3 (since $3^3 = 27 \equiv_{13} 1$), not 12.
(10 points) Find all complex solutions to $x^6 - 4x^3 + 3 = 0$. Which of these solutions are

(10 points) Show that for all odd k, $n^k - n$ is divisible by 3.

Proof. It is enough to show that $n^k - n \equiv_3 0$. If $n \equiv_3 0$ then clearly $n^k - n \equiv_3 0$. So we can assume $n \not\equiv_3 0$. Now we will use the fact that if $n \not\equiv_3 0$ then $n^2 \equiv_3 1$. Let $k = 2m+1$. Then $n^k - n = n^{2m+1} - n = n(n^2)^m - n \equiv_3 n(1)^m - n = n - n = 0$. So in either case, $n^k - n \equiv_3 0$.

(10 points) It happens to be true that 1997 and 1999 are both prime numbers (you don't have to check this). Explain why the polynomial $x^{1997} - 1$ has no roots in $\mathbb{Z}_{1999}$ other than $x = 1$. (Hint think about the order of the root.)

Solution. If there were such a root, its order would be exactly 1997 since 1997 has no divisors other than itself and 1. But any element of $\mathbb{Z}_{1999}$ satisfies the equation $x^{1998} - 1 \equiv_{1999} 0$, so its order divides 1998. Clearly 1997 does not divide 1998.

(15 points) Let a and b be nonzero integers such that $g = (a, b)$. Prove that $\left(\dfrac{a}{g}, \dfrac{b}{g}\right) = 1$.

Proof. Let $d = \left(\dfrac{a}{g}, \dfrac{b}{g}\right)$. Then $\dfrac{a}{g} = dh$ and $\dfrac{b}{g} = dk$ for some $h, k \in \mathbb{Z}$. Then $a = gdh$ and $b = gdk$. Hence gd is a common divisor of a and b. Since g is the greatest common divisor of a and b, we have $gd \leq g$. Both d and g are positive integers, forcing $d = 1$.

(15 points) For any prime p, if $a^p \equiv_p b^p$ then $a^p \equiv_{p^2} b^p$. (Hint: use Proposition 5.3.)

Proof. Suppose $a^p \equiv_p b^p$. By Fermat's theorem, $a \equiv_p a^p \equiv_p b^p \equiv_p b$. Hence as integers we have $a = b + kp$ for some integer k. This means that

$$a^p = (b+kp)^p = b^p + \binom{p}{1} b^{p-1}(kp) + \binom{p}{2} b^{p-2}(kp)^2 + \cdots .$$

Since $\binom{p}{1} = p$, the second term is $kb^{p-1}p^2$, which is divisible by p^2. All terms after that are of the form $\binom{p}{i} b^{p-i}(kp)^i$ for $i \geq 2$, so they are all divisible by p^2 as well. Hence $a^p - b^p$ is divisible by p^2, so $a^p \equiv_{p^2} b^p$.