**MATH 201 Solutions: TEST 3-A (in class)**

*Numbers are the highest degree of knowledge. It is knowledge itself.*

- Plato

P**art I** *[7 pts each]*

1. Carefully state the *Well-Ordering Principle*.

*The* ***well-ordering principle****states that every non-empty set of positive integers contains a least element.*

1. Carefully state the *Euclidean Division Algorithm*.

*Given two integers a and b, with b ≠ 0, there exist unique integers q and r such that*

*a = bq + r and 0 ≤  r < |b|.*

1. Define *gcd(a, b).*

*The* ***greatest common divisor*** *of two integers (not both zero) is the largest integer which divides both of them.*

*Equivalently, if a and b are not both zero, d = gcd(a, b) if the following two conditions are satisfied:*

1. *d|s and d|b*
2. *If e|a and e|b then |e| d*
3. State (the conclusion of) Euclid’s *extended gcd algorithm*.

*The conclusion of the* ***extended Euclidean algorithm****is:*

*If a and b are integers, not both 0, then there exist integers x and y such that*

*ax + by = gcd(a, b).*

1. Carefully state *Fermat’s little theorem*.

*If p is a prime number, then for any integer a,*

$a^{p}≡a (mod p)$*.*

*If a is not divisible by p,* ***Fermat's little theorem*** *is equivalent to the statement that*

$a^{p-1}≡1 \left(mod p\right).$

1. State *Euclid’s theorem* on prime numbers.

*There exist infinitely many primes.*

**Part II** *[10 pts each]*

1. Explain why every integer can be expressed in the form 5n, 5n+1, 5n+2, 5n+3 or 5n+4.

*It follows from Euclid’s division algorithm that every integer can be represented as 5q+ r,*

*where 0 r < 4.*

1. Using the Euclidean algorithm, find gcd(306, 657)

*gcd(306, 657) = gcd(657, 306) = gcd(45, 306) = gcd(306, 45) = gcd(36, 45) = gcd(45, 36) = gcd(9, 36) = gcd(36, 9) = gcd(0, 9) = gcd(9, 0) =* ***9***

1. Using the extended Euclidian algorithm, find integers *x* and *y* such that

56x + 22y = gcd(56, 22).

*First we use the Euclidean algorithm to find gcd(56, 22):*

*56 = 22 (2) + 12*

*22 = 12(1) + 10*

*12 = 10(1) + 2*

*10 = 2(5) + 0*

*So the gcd is 2.*

*Now, using back-substitution:*

*2 = 12 – 10(1)*

*= 12 – (22 – 12) = 2(12) – 22*

*= 2(56 – 22(2)) – 22 = 2(56) – 5 (22)*

*We conclude that an integer solution of 56x + 22y = gcd(56, 22)*

*is* ***x = 2*** *and* ***y = -5****.*

1. Prove that gcd(a, b – a) = gcd(a, b).

*Let d = gcd(a, b – a) and d\* = gcd(a, b).*

*Now d|a and d| (b – a) by definition of gcd.*

*So d| {a + (b – a)} = b*

*Thus d|a and d| b. So, by definition of gcd, |d| |d\*|*

*Next, d\*|a and d\*|b. So, d\*| ((-1) a + b) d\* | b – a.*

*Thus |d\*| |d|.*

*So we arrive at |d\*| = |d|. Of course, d and d\* are each positive, so d\* = d.*

1. Using Fermat’s little theorem find 5101 (mod 31)

*Since 31 is a prime and not a factor of 5, Fermat’s little theorem states 530 1 (mod 31).*

*And so 590 = (530)3 13 = 1 (mod 31).*

*Next 5101 = 590 511  511 (mod 31).*

*Note that 53 = 125 = 4(31) + 1 1 (mod 31).*

*Finally, 5101 511 = (53)3 52 13 25 =* ***25*** *(mod 31).*

1. The converse to Fermat’s little theorem is false. Namely:

If am-1 1 mod m, it need not follow that *m* is prime.

1. *[7 pts]* Find 2560 mod 561

*First, note that 210 463 (mod 561).*

*So 220 =(210)2 4632 67 (mod 561)*

*So 240 =(220)2 672 1 (mod 561)*

*Finally, 2560 = (240)14 114 = 1 (mod 561)*

(b) *[3 pts]* Show that 561 is not a prime number. (Such numbers are called *pseudo-primes*.)

*Since 3|561, 561 cannot be prime.*

1. Prove that if a|b and c|d then ac|bd.

*Since a| b m Z such that b = am.*

*Since c|d n Z such that d = cn.*

*Thus bd = (am) (cn) = (ac) (mn). Of course mn Z.*

*Hence ac|bd.*

1. Prove that $\sqrt{3 }$ is irrational.

*Suppose, contrary to fact, that that* $\sqrt{3 }$ *is rational. Then a, b Z, b 0 , such that*

$\sqrt{3 } $*= a/b.*

*We may assume that a and b are relatively prime. (If not, divide each of a and b by gcd(a, b).)*

*So a2 = 3b2. Hence a2 is a multiple of 3. This implies that a is a multiple of 3. (Examine the three cases: a = 3p, a = 3p+1, a = 3p+2.)*

*Hence q Z such that a = 3q.*

*So 3b2 = a2 = (3q)2 = 9q2.*

*From this, we obtain: b2 = 3q2. As argued earlier, this implies that b is a multiple of 3.*

*This is clearly a contradiction, since if a and b were divisible by 3, then a and b would not be relatively prime, as we assumed above.*

1. Prove that the *square of any integer* is either of the form 3k or 3k+1.

*Using the division algorithm, every integer, n, may be expressed as*

*n = 3z + r where r = 0, 1, 2.*

*Examining each of these three cases:*

*(3z)2 = 3(3z2)*

*(3z + 1)2 = 9z2 + 6z + 1 = 3(3z2 + 2z) + 1*

*(3z + 2)2 = 9z2 + 12z + 4 = 3(3z2 + 4z + 1) + 1*

*Thu,s for each of the three cases, n2 is either of the form 3k or 3k+1.*

Extra credit:

1. *[10 pts]* Prove by induction: For n N, if an|bn then a|b.

*For each n N, let Hn represent the statement: if an|bn then a|b.*

***Base Case:*** *H1 is true since if a1|b1 then clearly a|b.*

***Inductive step:*** *Let n 0 be given. Assume that an+1|bn+1.*

*Let d = gcd(a, b). Let A = a/d and B = b/d. We have proven earlier that A and B are relatively prime. Now, an+1|bn+1 implies that An+1|Bn+1.*

*It is easy to show that An+1 and Bn+1 are relatively prime.*

*Rewriting: AAn | BBn*

*Then, by Euclid’s lemma, since A and B are relatively prime, An|B or An |Bn.*

*If An |Bn, then we can use the inductive hypothesis to conclude that A|B and hence a|b.*

*If An | B, then of course A|B.*

1. *[10 pts]* Prove that (3n)!/(3!)n is an integer for all n 0. (Recall that 0! = 1)

*For each n 0, let Hn represent the statement: if an|bn then a|b.*

***Base case:*** *n = 0: (3(0))!/(3!)0 == 1 Z.*

***Inductive step:*** *Assume that n 0 is given and that Hn is true.*

*Now (3(n+1))!/(3!)n+1 = (3n + 3)! / (3!)n+1* $=\left(\frac{\left(3n\right)!}{\left(3!\right)^{n}}\right) \left(\frac{\left(3n+1\right)\left(3n+2\right)\left(3n+3\right)}{3!}\right)=$

$\left(\frac{\left(3n\right)!}{\left(3!\right)^{n}}\right)(n+1)\frac{(3n+1)(3n+2)}{2}$

*Now, by inductive hypothesis,* $\left(\frac{\left(3n\right)!}{\left(3!\right)^{n}}\right) $*is an integer. Furthermore, the product of two consecutive integers is even. Thus (3n+1)(3n+2) is divisible by 2.*

*So we have shown that Hn+1 is true.*