Dalhousie University, MATH 3070
Midterm # 1 Solutions
Tuesday, October 7, 2008

1. Prove or disprove the following.

   (a) [5] *The sum of any two prime numbers is composite.*
   False: $2 + 3 = 5$.

   (b) [5] *Let $d = \gcd(a, b)$. Then for any $m, n \in \mathbb{N}$, $\gcd(a^m, b^n) = d^{\min(m,n)}$.*
   False: let $a = b^2$ and $m = 1, n = 2$. Then $d = b$ but $\gcd(a, b^2) = b^2 \neq d^{\min(1,2)}$.

   (c) [5] *Let $a, m, k, \ell$ be positive integers such that $a^k \equiv a^\ell \equiv 1 \pmod{m}$. Then $a^{\gcd(k,\ell)} \equiv 1 \pmod{m}$.*
   True: Let $d = \gcd(k, \ell) = kx + \ell y$ for some integers $x, y$. Then $a^d = a^{kx+\ell y} = (a^k)^x (a^\ell)^y \equiv 1^x 1^y \equiv 1 \pmod{m}$.

   (d) [5] *For $n \geq 3$, $n^n$ is never congruent to $2 \pmod{n+1}$.*
   True: For any $n$, $n^n \equiv (-1)^n \equiv \pm 1 \pmod{n+1}$. But if $n \geq 3$ then $2 \not\equiv \pm 1 \pmod{n+1}$.

2. (a) [5] *Let $p$ be a prime. Prove that if $(a, p) = 1$, then $a^{p^n - 1} \equiv 1 \pmod{p}$.*
   By Fermat's little theorem, if $(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod{p}$.
   Thus $a^{p^n-1} = a^{(p-1)(1+p+\cdots+p^{n-1})} \equiv 1^{1+p+\cdots+p^{n-1}} \equiv 1 \pmod{p}$.
   Alternate solution: By Fermat's little theorem, we have $a^p \equiv a \pmod{p}$ for all $a$.
   Thus $a^{p^n} = (a^{p^{n-1}})^p \equiv a^{p^{n-1}} \equiv \cdots \equiv a \pmod{p}$. Thus if $(a, p) = 1$ then $a$ is invertible mod $p$ so $a^{p^n} a^{-1} = a^{p^n - 1} \equiv 1 \pmod{p}$.

   (b) [5] *Prove that $4^n \equiv 1 + 3n \pmod{9}$ for all $n \in \mathbb{N}$.*
   Write $4^n = (1 + 3)^n = 1 + 3n + 3^2 \binom{n}{2}$ + terms involving higher powers of 3. Thus $4^n \equiv 1 + 3n \pmod{9}$.
   Alternate solution: Induct on $n$. Base case $n = 0$ reduces to $1 \equiv 1 \pmod{9}$. Now suppose $4^n \equiv 1+3n \pmod{9}$. Then $4^{n+1} \equiv (1+3n)4 = 4+12n \equiv 1+3+3n = 1+3(n+1) \pmod{9}$.

3. (a) [5] *Prove that any integer of the form $8k + 7$ is not expressible as a sum of three squares.*
   We reduce mod 8. We find that for any $x$, $x^2 \equiv 0, 1, 4 \pmod{8}$. Thus the possible classes for $x^2 + y^2 + z^2 \pmod{8}$ are:

$$\begin{aligned}
0 + 0 + 0 &\equiv 0 \pmod{8} \\
0 + 0 + 1 &\equiv 1 \pmod{8} \\
0 + 0 + 4 &\equiv 4 \pmod{8} \\
0 + 1 + 1 &\equiv 2 \pmod{8} \\
0 + 1 + 4 &\equiv 5 \pmod{8} \\
0 + 4 + 4 &\equiv 0 \pmod{8} \\
1 + 1 + 1 &\equiv 3 \pmod{8} \\
1 + 1 + 4 &\equiv 6 \pmod{8} \\
1 + 4 + 4 &\equiv 1 \pmod{8} \\
4 + 4 + 4 &\equiv 4 \pmod{8}
\end{aligned}$$

   which is never $7 \pmod{8}$.

(b) [10] *Prove that any integer of the form $4^n(8k+7)$ is not expressible as a sum of three squares. (Hint: if $x^2+y^2+z^2 = 4^n(8k+7)$, what can you say about the parity of $x$, $y$, and $z$?)*

We induct on $n$. The base case $n = 0$ is part a. Note that we have $4(8k+7) \equiv 4 \pmod 8$ and $4^n(8k+7) \equiv 0 \pmod 8$ if $n \geq 2$. In either case, from the table above we find that all three of $x^2, y^2$, and $z^2$ are even and so $x, y$, and $z$ must all be even. Thus if there is a solution $(x, y, z)$ for some $n \geq 1$, then we my rewrite $x = 2X, y = 2Y, z = 2Z$ and obtain an equation

$$4X^2 + 4Y^2 + 4Z^2 = 4^n(8k+7)$$

Dividing out the 4 on both sides yields $(X, Y, Z)$ as a solution to the equation $X^2+Y^2+Z^2 = 4^{n-1}(8k+7)$, contradicting the inductive hypothesis.

4. [10] *Bob the pirate wants to retire and decided to divide up his crew among his 5 children. Unfortunately, he found that if he split his crew up evenly, then there would be 3 crewmen leftover, but if he had one more child then they would divide up evenly. Since his crew is part of a powerful pirate's union, he can't just fire (his gun at) three random people. So Bob decided to have another kid. Much to his dismay, 9 months later his wife gave birth to twins! Now, if he divided up his crew evenly among his 7 children, he would have 5 leftover! What is the least number of crewmen Bob has in order for him to be caught in this situation?*

Let $x$ be the number of crewmen. Then $x$ must satisfy the system of congruences

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 0 \pmod 6 \\ x &\equiv 5 \pmod 7. \end{aligned}$$

The second congruence means $x = 6x_1$. Plugging it into the 3rd congruence we have $6x_1 \equiv 5 \equiv 12 \pmod 7$ so $x_1 \equiv 2 \pmod 7$. Thus $x = 6x_1 = 6(7x_2+2) \equiv 3 \pmod 5$. Simplifying, we find that $2x_2 \equiv 1 \pmod 5$ so $x_2 \equiv 3 \pmod 5$. Thus we have $x = 6(7(5x_3+3)+2) = 210x_3 + 6(23) = 210x_3 + 138$. So the minimum number of crewmen is 138.

5. [10] *Suppose you have two containers: one holds 591 mL and the other holds 1890 mL. By filling one and emptying it into the other, you can measure any (integral) linear combination of their volumes. Is it possible to use them to measure out 15 mL of water?*

We want to know whether $591x + 1890y = 15$ has a solution in integers $x$ and $y$. Applying the Euclidean algorithm, we find that

$$\begin{aligned} 1890 &= 3(591) + 117 \\ 591 &= 5(117) + 6 \end{aligned}$$

and $\gcd(117, 6) = 3$. So there is a solution to $591x' + 1890y' = 3$. Let $x = 5x'$ and $y = 5y'$ yields a solution to $591x + 1890y = 15$.

6. [10] *Let $a, b \in \mathbb{N}$. Prove that if $1/a + 1/b \in \mathbb{N}$ then $a = b$. In this case determine the possible values of $a$.*

If $1/a + 1/b \in \mathbb{N}$ then $(a+b)/ab \in \mathbb{N}$ so $ab|(a+b)$. In particular, $a|(a+b)$ and so $a|b$. Similarly, $b|(a+b)$ so $b|a$. Therefore $b = \pm a$. But since both $a$ and $b$ are positive we must have $a = b$.

In this case, we have $1/a + 1/b = 2/a \in \mathbb{N}$. Therefore $a|2$ so $a = 1$ or $a = 2$.

7. [5] *Let $p$ be a prime and let $H_p := 1 + 1/2 + \cdots + 1/p$ be the $p$th Harmonic number. Prove that when $H_p$ is written as a rational $a/b$ in lowest terms, the numerator $a$ satisfies $(a, p) = 1$ and the denominator $b \equiv 0 \pmod{p}$. Hence $H_p$ is not an integer.*

Putting everything under a common denominator, we find that

$$H_p = \frac{p! + p!/2 + p!/3 + \cdots + p!/p}{p!} = \frac{p((p-1)! + \frac{(p-1)!}{2} + \cdots + \frac{(p-1)!}{p-1}) + (p-1)!}{p!}.$$

Thus $H_p = (pk + (p-1)!)/p!$ for some integer $k$, before we reduce it into lowest terms. But since the numerator in this case is $-1 \pmod{p}$ by Wilson's Theorem, it is already coprime to $p$ and cancelling out factors from the denominator will not introduce $p$'s in the numerator. Thus $(a, p) = 1$. Also, since the numerator in the unreduced form is already coprime to $p$, the $p$ in the denominator does not cancel and thus remains in $b$ when reduced to lowest terms. Therefore $b \equiv 0 \pmod{p}$.