Math 320 - Dr. Miller - Solutions to Final Exam - May 6, 2008

1. *[10 pts]* Find all pairs of positive integers a and b for which $(a, b) = 17^2 \cdot 19$ and $[a, b] = 13 \cdot 17^3 \cdot 19^2$. Show clear work.

Because $(a, b) = 17^2 \cdot 19$ is a common factor, both numbers must contain this prime factorization. The remaining prime factors of $[a, b] = 13 \cdot 17^3 \cdot 19^2$ – namely, the extra 13, 17, and 19 – can be shared between a and b in any combination. Thus, we obtain these options:

$$\begin{aligned} a &= 17^2 \cdot 19 & b &= 13 \cdot 17^3 \cdot 19^2 \\ a &= 13 \cdot 17^2 \cdot 19 & b &= 17^3 \cdot 19^2 \\ a &= 17^3 \cdot 19 & b &= 13 \cdot 17^2 \cdot 19^2 \\ a &= 17^2 \cdot 19^2 & b &= 13 \cdot 17^3 \cdot 19. \end{aligned}$$

2. *[10 pts]* Solve the congruence $575x \equiv 5$ *mod* 1720. Show clear work.

$$\begin{array}{rccl} 575x & \equiv & 5 & mod\ 1720 \\ \div 5 & & \div 5 & \div(1720, 5) \\ 115x & & 1 & mod\ 344 \\ \times 3 & & \times 3 & \\ x & \equiv & 3 & mod\ 344 \end{array}$$

$$x \equiv 3,\ 347,\ 691,\ 1035,\ 1379\ mod\ 1720$$

3. *[15 pts]* Solve this system of congruences by your choice of method, showing clear work:

$$\begin{aligned} x &\equiv 1 \quad mod\ 5 \\ x &\equiv 2 \quad mod\ 6 \\ x &\equiv 3 \quad mod\ 7 \end{aligned}$$

Applying the proof technique for the Chinese Remainder Theorem produces this solution: Our final modulus is $M = 5 \cdot 6 \cdot 7 = 210$. The first term of the solution formula requires $M_1 = 6 \cdot 7 = 42$, and we find its inverse x_1 mod 5 via

$$42x_1 \equiv 1 \quad mod\ 5 \Longrightarrow 2x_1 \equiv 1 \Longrightarrow 3(2x_1) \equiv 3(1) \Longrightarrow x_1 \equiv 3 \quad mod\ 5.$$

The second term requires $M_2 = 5 \cdot 7 = 35$, and its inverse x_2 mod 6:

$$35x_2 \equiv 1 \quad mod\ 6 \Longrightarrow -x_2 \equiv 1 \Longrightarrow x_2 \equiv -1 \Longrightarrow x_2 \equiv 5 \quad mod\ 6.$$

The third and final term requires $M_3 = 5 \cdot 6 = 30$, *and its inverse* x_3 *mod* 7*:*

$$30x_3 \equiv 1 \quad mod\ 7 \Longrightarrow 2x_3 \equiv 1 \Longrightarrow 4(2x_3) \equiv 4(1) \Longrightarrow x_3 \equiv 4 \quad mod\ 7.$$

The solution is

$$x = (1)(42)(3) + (2)(35)(5) + (3)(30)(4) = 836 \equiv 206 \quad mod\ 210.$$

Applying back-substitution produces this solution:

$$\begin{array}{lll}
x \equiv 1 \quad mod\ 5 & \Longrightarrow & x = 5k+1\ for\ some\ k \in \mathbf{Z} \\
x \equiv 2 \quad mod\ 6 & \Longrightarrow & 5k+1 \equiv 2 \quad mod\ 6 \\
 & \Longrightarrow & 5k \equiv 1 \quad mod\ 6 \\
 & \Longrightarrow & 5(5k) \equiv 5(1) \quad mod\ 6 \\
 & \Longrightarrow & k \equiv 5 \quad mod\ 6 \\
 & \Longrightarrow & k = 6m+5\ for\ some\ m \in \mathbf{Z} \\
 & \Longrightarrow & x = 5(6m+5)+1 = 30m+26\ for\ some\ m \in \mathbf{Z} \\
x \equiv 3 \quad mod\ 7 & \Longrightarrow & 30m+26 \equiv 3 \quad mod\ 7 \\
 & \Longrightarrow & 2m-2 \equiv 3 \quad mod\ 7 \\
 & \Longrightarrow & 2m \equiv 5 \quad mod\ 7 \\
 & \Longrightarrow & 4(2m) \equiv 4(5) \quad mod\ 7 \\
 & \Longrightarrow & m \equiv 20 \equiv 6 \quad mod\ 7 \\
 & \Longrightarrow & m = 7n+6\ for\ some\ n \in \mathbf{Z} \\
 & \Longrightarrow & x = 30(7n+6)+26 = 210n+206\ for\ some\ n \in \mathbf{Z} \\
 & \Longrightarrow & x \equiv 206 \quad mod\ 210
\end{array}$$

4. *[10 pts]* Find the least nonnegative residue of each number below. Show clear work; indicate how you apply any named theorems.

   (a) 23^{33} mod 31

   Because 31 *is prime and* $23 \in \mathbf{Z}$, *we apply the corollary to Fermat's Little Theorem to see that* $23^{31} \equiv 23$ *mod* 31*. Then* $23^{33} \equiv 23^{31} \cdot 23^2 \equiv 23^3 = 12167 \equiv 15$ *mod* 31*.*

   (b) 23^{33} mod 48

   Because $(23, 48) = 1$ *and* $\phi(48) = \phi(2^4 \cdot 3) = \phi(2^4) \cdot \phi(3) = (2^4 - 2^3)(2) = 2^4 = 16$, *we apply Euler's Theorem to see that* $23^{16} \equiv 1$ *mod* 48*. Then* $23^{33} = (23^{16})^2 \cdot 23 \equiv 1 \cdot 23 = 23$ *mod* 48*.*

5. *[10 pts]* Find three solutions with $x \geq 0$ for the diophantine equation $45x + 75y = 210$.

The gcd of 45 *and* 75 *is* 15*, and we can write* $45(2) + 75(-1) = 15$*. Multiplying this equality by 14 yields* $45(28) + 75(-14) = 210$*. We can now add and subtract the lcm of* 45 *and* 75*, which is* 225*, to obtain further solutions. Those solutions having* $x \geq 0$ *are listed in increasing order of* x *below:*

$$\begin{array}{rl} x = 3 & y = 1 \\ x = 8 & y = -2 \\ x = 13 & y = -5 \\ x = 18 & y = -8 \\ x = 23 & y = -11 \\ x = 28 & y = -14 \\ x = 33 & y = -17 \\ x = 38 & y = -20 \\ \vdots & \vdots \end{array}$$

6. *[10 pts]* Find one primitive and two nonprimitive Pythagorean triples involving the number 85. Show clear work.

There is one primitive triple for which $85 = m^2 + n^2$ *– namely, when* $m = 7$ *and* $n = 6$*. This yields a triple of* $x = 7^2 - 6^2 = 13$*,* $y = 2(7)(6) = 84$*,* $z = 85$*. There is also at least one triple for which* $85 = m^2 - n^2$ *– namely, when* $m = 43$ *and* $n = 42$ *– yielding* $x = 85$*,* $y = 2(43)(42) = 3612$*,* $z = 43^2 + 42^2 = 3613$*. So the most immediate primitive triples are*

$$(13, 84, 85) \quad \textit{and} \quad (85, 3612, 3613).$$

Nonprimitive triples can be built upon triples involving the factors 5 *or* 17 *of* 85*. For* 5*, the familiar triple of* $(3, 4, 5)$*, the only one having* $5 = m^2 + n^2$*, can be multiplied by* 17*, or the other primitive triple* $(5, 12, 13)$ *– in which* $5 = 2^2 + 1^2$*, and the only one expressing* 5 *as a difference of squares – can be similarly multiplied. For* 17*, we may use either the triple* $(15, 8, 17)$ *– where* $m = 4$ *and* $n = 1$*, and the only one having* $17 = m^2 + n^2$ *– or* $(17, 144, 145)$*, having* $m = 9$ *and* $n = 8$*, unique in having* $17 = m^2 - n^2$*. Each can be multiplied by* 5*. Thus, the only nonprimitive triples involving* 85 *are*

$$(51, 68, 85), \quad (85, 204, 221), \quad (75, 40, 85), \quad \textit{and}\ (85, 720, 725).$$

7. *[10 pts]* Define an arithmetic function $f(n) = \sum_{d|n, d>0} \sigma(d)$. Compute $f(18)$.

$$f(18) = \sigma(1) + \sigma(2) + \sigma(3) + \sigma(6) + \sigma(9) + \sigma(18) = 1 + 3 + 4 + 6 + 13 + 39 = 66$$

8. *[15 pts]* Let n be an integer that is not divisible by 7. Prove that if $n^3 \equiv n \bmod 21$, then n is its own inverse mod 7.

By definition of congruence, we have that $21 \mid n^3 - n$. *By transitivity, then (since* $7 \mid 21$*),* $7 \mid n^3 - n$, *which factors as* $n(n^2 - 1)$. *because 7 is prime, it must divide* n *or* $n^2 - 1$, *yet by assumption, it does not divide* n. *Therefore,* $7 \mid n^2 - 1$, *whence* $n^2 \equiv 1$ *mod 7, showing that* n *is its own inverse mod 7.*

9. *[15 pts]* Let $a, b, c \in \mathbf{Z}$. Prove that $(a, c) = (b, c) = 1$ if and only if $(ab, c) = 1$.

$\Longrightarrow$: *Let* $(a, c) = (b, c) = 1$. *By alternative definition, there exist integers* x, y, z, w *such that* $ax + cy = 1$ *and* $bz + cw = 1$. *Multiplying these two equalities creates* $(ax+cy)(bz+cw) = 1$, *or* $ab(xz)+c(axw+byz+xyw) = 1$. *Since* $xz, axw+byz+xyw \in \mathbf{Z}$ *by closure, we have an integer linear combination of* ab *and* c *that equals 1, whence* $(ab, c) = 1$.

$\Longleftarrow$: *Assume that* $(ab, c) = 1$. *By alternative definition, there exist* $p, q \in \mathbf{Z}$ *with* $abp + cq = 1$. *Rewriting this equality as* $a(bp) + cq = 1$ *shows that* $(a, c) = 1$, *for* $bp \in \mathbf{Z}$ *by closure and* $q \in \mathbf{Z}$ *by assumption. Similarly,* $(b, c) = 1$ *from* $b(ap) + cq = 1$ *with* $ap \in \mathbf{Z}$ *by closure and* $q \in \mathbf{Z}$ *by assumption.*

10. *[15 pts]* Prove that if n is a positive integer greater than 1, then n has a prime factorization.

Suppose to the contrary that there exist integers greater than 1 having no prime factorization. By the Well-Ordering Principle, there exists a smallest such integer; call it n. *We see that* n *cannot be prime, for then it would be its own prime factorization. Thus,* n *is composite and can be expressed as* $n = ab$ *where* $1 < a, b < n$. *Because* n *is the smallest integer greater than 1 that lacks a prime factorization, both* a *and* b *must have one. But then their product* n *may be expressed as the product of their prime factorizations, creating one for* n. *By contradiction, then, no* n *as described can exist, so that every integer greater than 1 has a prime factorization.*

11. *[15 pts]* Let p and $p - 4$ be primes. Prove that $4(p-1)! - p \equiv -4 \bmod p(p-4)$.

Consider the congruence mod p *alone first. By Wilson's Theorem, since* p *is prime, we have that* $(p-1)! \equiv -1$ *mod* p. *Then*

$$4(p-1)! - p \equiv 4(-1) - 0 \equiv -4 \quad \textit{mod } p.$$

Next consider the congruence mod $p-4$ *alone. Then* $p-1)! = (p-1)(p-2)(p-3)(p-4)(p-5)! \equiv (p-1)(p-2)(p-3)\cdot 0 \cdot (p-5)! = 0$ *mod* $p-4$*, whence*

$$4(p-1)! - p \equiv 0 - (+4) \equiv -4 \quad mod\ p-4.$$

Because p *and* $p-4$ *are prime, they are relatively prime to each other, so that because the congruence holds true for each separately, it is also true mod* $p(p-4)$.

12. *[15 pts]* Let $n \in \mathbf{Z}^+$. Prove that $\phi(\phi(3^n)) = \frac{2}{3}\phi(3^n)$.

Note that

$$\begin{aligned}
\phi(\phi(3^n)) &= \phi(3^n - 3^{n-1}) \\
&= \phi(3^{n-1}(3-1)) \\
&= \phi(3^{n-1}\cdot 2) \\
&= (3^{n-1} - 3^{n-2})\cdot 1 \\
&= 3^{n-1}(1-\frac{1}{3})\cdot 1 \\
&= \frac{2}{3}\cdot 3^{n-1}
\end{aligned}$$

(Observe that $n \geq 2$ *else* $\phi(3^{n-1})$ *is undefined.) Now*

$$\begin{aligned}
\frac{2}{3}\phi(3^n) &= \frac{2}{3}(3^n - 3^{n-1}) \\
&= \frac{2}{3}\cdot 3^{n-1}(3-1) \\
&= \frac{4}{3}\cdot 3^{n-1}
\end{aligned}$$

Oops! These two formulae are not equal, so the result is not confirmed. The correct formula should have had a coefficient of $\frac{1}{3}$*, not* $\frac{2}{3}$.