Math 320 - Dr. Miller - Solutions to Exam #1 - Feb. 18, 2008

1. *[8 pts]* Precisely state the Division Algorithm, then provide the guaranteed conclusions when $a = -514$ and $b = 63$.

   Theorem (Division Algorithm): Let $a, b \in \mathbf{Z}$ with $b > 0$. Then there exist unique integers q and r with $a = bq + r$ and $0 \leq r < b$.

   Computationally, we must "undershoot" -514 with a multiple of 63 to get the desired behavior for our remainder. Because $63 \cdot (-8) = -504$, we must consider $63 \cdot (-9) = 567$. Then $-514 = 63 \cdot (-9) + 53$, where $0 \leq 53 < 63$. Let $q = -9$ and $r = 53$.

2. *[8 pts]* Precisely state the definition of "Mersenne prime," then provide an example of twin primes p and q where p is a Mersenne prime. Justify this condition on p.

   Definition: A Mersenne prime is a prime number of the form $2^p - 1$ where p is also a prime.

   The twin primes 3 and 5 have $p = 3$ a Mersenne prime, for $3 = 2^2 - 1$ and the exponent 2 is prime.

3. *[8 pts]* Precisely state Goldbach's Conjecture, then verify it for 28.

   Goldbach's Conjecture: Every even integer greater than 2 can be expressed as the sum of two primes.

   The expression $28 = 11 + 17$ satisfies this claim.

4. *[8 pts]* Create a list of six consecutive composite numbers, indicating an appropriate divisor for each.

   Consider the sequence $7! + 2, 7! + 3, 7! + 4, 7! + 5, 7! + 6, 7! + 7$. (These are the integers $5042, 5043, 5044, 5045, 5046, 5047$.) By creation, we have

$$\begin{aligned} 2 &\mid 7! + 2 \\ 3 &\mid 7! + 3 \\ 4 &\mid 7! + 4 \\ 5 &\mid 7! + 5 \\ 6 &\mid 7! + 6 \\ 7 &\mid 7! + 7. \end{aligned}$$

5. *[8 pts]* Find all pairs of positive integers a and b for which $(a, b) = 50$ and $[a, b] = 1500$.

Factor $(a, b) = 2 \cdot 5^2$ and $[a, b] = 2^2 \cdot 3 \cdot 5^3$. Each of a and b must contain the shared factors 2 and 5^2. We must distribute the remaining factors of 2, 3, and 5 in all possible ways. The options are below:

$$\begin{aligned} 2 \cdot 5^2 &= 50 \quad \textit{and} \quad 2^2 \cdot 3 \cdot 5^3 = 1500 \\ 2^2 \cdot 5^2 &= 100 \quad \textit{and} \quad 2 \cdot 3 \cdot 5^3 = 750 \\ 2 \cdot 3 \cdot 5^2 &= 150 \quad \textit{and} \quad 2^2 \cdot 5^3 = 500 \\ 2 \cdot 5^3 &= 250 \quad \textit{and} \quad 2^2 \cdot 3 \cdot 5^2 = 300 \end{aligned}$$

6. *[15 pts]* Prove rigorously that if a and b are integers with $a^2 \mid b$ and $b^2 \mid a$, then a must equal 0, 1, or -1.

Assume that $a^2 \mid b$ and $b^2 \mid a$ for some $a, b \in \mathbf{Z}$. Then there exist integers x and y for which $a^2 x = b$ and $b^2 y = a$. Substituting the first equation into the second yields $(a^2 x)^2 y = a$, or

$$a^4 x^2 y = a.$$

Certainly, this is true if $a = 0$. If not, we may divide both sides by a to obtain $a^3 x^2 y = 1$. Yet this equality can be true for integers a, x, and y only if they are all ± 1, as desired.

7. *[15 pts]* Given integers a and b, not both zero, prove that the smallest member d of the set below is a common divisor of a and b.

$$S = \{ax + by \mid x, y \in \mathbf{Z} \text{ and } ax + by > 0\}$$

We know that $d = ax + by$ for some $x, y \in \mathbf{Z}$. Because $a, d \in \mathbf{Z}$ with $d > 0$, we may apply the Division Algorithm to obtain $a = dq + r$ where $q, r \in \mathbf{Z}$ and $0 \leq r < d$. Then

$$r \;=\; a - dq \;=\; a - (ax + by)q = a(1 - qx) + b(-qy),$$

which, if positive, belongs to S since $1 - qx$ and $-qy$ are integers by closure. Yet $r < d$ would contradict the fact that d is the smallest member of S; therefore, we cannot have $r > 0$. Then $r = 0$ implies that $a = dq$, whence $d \mid a$ since $q \in \mathbf{Z}$. Similarly, $d \mid b$, and d is a common divisor, as desired.

8. *[15 pts]* Recall that every integer greater than 1 has a prime factor. Prove carefully that if n is composite, then n has a prime divisor p with $p \leq \sqrt{n}$.

Let n be a composite number. Then $n = ab$ where $a, b \in \mathbf{Z}$ with $1 < a, b < n$. Now one of a or b must be less than or equal to $\sqrt{n}$, for if not, then $ab > \sqrt{n} \cdot \sqrt{n} = n$, a contradiction. Without loss of generality, let $a \leq \sqrt{n}$. By hypothesis, a has a prime factor p (because a is an integer greater than 1). Also $a \mid n$ since b is an integer. Then by transitivity, $p \mid a$ and $a \mid n$ implies that $p \mid n$. Because $p \leq a < \sqrt{n}$, we have the desired inequality.

9. *[15 pts]* Prove rigorously that if $a, b, c \in \mathbf{Z}$ with $(a, b) = 1$ and $c \mid a + b$, then $(a, c) = (b, c) = 1$.

Because $(a, b) = 1$, there exist integers m and n with $1 = am + bn$. Now $c \mid (a + b)$ implies that there is an integer x for which $cx = a + b$. By algebra, we obtain $a = cx - b$. Substituting into our first equation yields $1 = (cx - b)m + bn = cxm + b(n - m)$. Because xm and $n - m$ are integers by closure, we have a linear combination of c and b resulting in 1, whence $(b, c) = 1$ by alternative definition of relative primality. Similarly, because the equation $cx = a + b$ is symmetric in a and b, we have that $(a, c) = 1$.