

Math 567 Fall 2008, Number Theory I, Solutions 1

1. Given $a|b$ and $c|d$, prove that $ac|bd$. By definition there are $u, v \in \mathbb{Z}$ such that $b = au$, $d = cv$. Thus $bd = aucv = (ac)(uv)$.

2. Prove that if n is odd, then $n^2 - 1$ is divisible by 8. Since n is odd, $n = 4k + r$ with $r = 1$ or 3 . Then $n^2 - 1 = 16k^2 + 8kr + r^2 - 1$ and in either case $8|r^2 - 1$.

3. Find the greatest common divisor g of the numbers 1819 and 3587, and then find integers x and y to satisfy $1819x + 3587y = g$. $3587 = 1819 \cdot 1 + 1768$, $1819 = 1768 \cdot 1 + 51$, $1768 = 51 \cdot 34 + 34$, $51 = 34 \cdot 1 + 17$, $34 = 17 \cdot 2 + 0$. Thus $g = 17 = 51 - 34 = 51 - (1768 - 41 \cdot 34) = 35(1819 - 1768) - 1768 = 1819 \cdot 35 - (3587 - 1819) \cdot 36 = 1819 \cdot 71 - 3587 \cdot 36$. $x = 71$, $y = -36$.

4. Let $g > 0$ and b be given integers. Prove that the equations $(x, y) = g$ and $xy = b$ can be solved simultaneously if and only if $g^2|b$. Suppose first that $(x, y) = g$ and $xy = b$. Then $g|x$, $g|y$ and so $g^2|b$. Suppose second that $g^2|b$. Let $x = g$, $y = b/g$. Then $g|y$, $g|(x, y) = (g, y)|g$.

5. Prove that every positive integer is uniquely expressible in the form $2^{j_0} + 2^{j_1} + 2^{j_2} + \dots + 2^{j_m}$ where $m \geq 0$ and $0 \leq j_0 < j_1 < j_2 < \dots < j_m$. We first prove by induction on k that there is always such a representation when $n < 2^k$. The case $k = 1$ is trivial. Now suppose that the inductive hypothesis holds and that $2^k \leq n < 2^{k+1}$. If $n = 2^k$ we are done so we can suppose that $2^k < n < 2^{k+1}$. Now $0 < n - 2^k < 2^k$ and by the inductive hypothesis $n - 2^k$ has a representation, and $2^{j_m} \leq n - 2^k < 2^k$. To prove uniqueness we need only consider a representation in which j_m is minimal. Then $n \leq 1 + 2 + \dots + 2^{j_m} < 2^{j_m+1}$. Thus no representation can have a larger power of 2 than 2^{j_m} , and so by the minimality of j_m all representations have 2^{j_m} as largest power of 2. Now one can consider $n - 2^{j_m}$ and proceed by induction on n .

6. Prove that there are no positive integers a, b, n with $n > 1$ such that $(a^n - b^n)|(a^n + b^n)$. Without loss of generality we can suppose that $a > b$ ($a = b$ would imply $0|a^n - b^n$). Suppose there is such a solution. Then by taking out common factors we can suppose that $(a, b) = 1$. Clearly $a^n - b^n|a^n + b^n + a^n - b^n = 2a^n$ and $a^n - b^n|a^n + b^n - a^n + b^n = 2b^n$. Hence $a^n - b^n|(2a^n, 2b^n) = 2$. Thus $a^n - b^n = 1$ or 2 . But $a \geq b + 1$, so $a^n - b^n \geq (b + 1)^n - b^n = (b + 1 - b)((b + 1)^{n-1} + (b + 1)^{n-2}b + \dots + b^{n-1}) \geq b + 1 + (n - 1)b \geq 2 + n - 1 = n + 1 > 2$.

7. Prove that any positive integer of the form $4k + 3$ has a prime factor of the same form, and similarly for the form $6k + 5$. Deduce that there are infinitely many primes of the form $4k + 3$ and similarly for $6k + 5$. All prime factors of $4k + 3$ must be odd so are of the form $4k' + r$ with $r = 1$ or $r = 3$. Since $(4k_1 + 1)(4k_2 + 1) = 16k_1k_2 + 4(k_1 + k_2) + 1$ is of the form $4k' + 1$ it easily follows that there is a prime factor of $4k + 3$ of the same form. Suppose that there are only a finite number of primes of this form, say $3, 7, 11, \dots, p_j$. Let $k = 7 \cdot 11 \dots p_j$. The $4k + 3$ has a prime factor p of the form $4k' + 3$. If $p = 3$, then $p|4k$ which is impossible. If $p > 3$, then $p|k$ and so $p|3$ which is also impossible.

Obviously $6k + 5$ can have no factor of the form $6k' + r$ with $r = 0, 2, 3$ or 4 . Then much as above not all the prime factors can be of the form $6k' + 1$. Finally we can suppose $k = 11 \cdot 17 \dots p_j$, etcetera.