MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2024, SOLUTIONS 2

1. Let $a, b, c \in \mathbb{Z}$. Prove each of the following.

(i) $a|a$. (ii) If $a|b$ and $b|a$, then $a = \pm b$. (iii) If $a|b$ and $b|c$, then $a|c$. (iv) If $ac|bc$ and $c \neq 0$, then $a|b$. (v) If $a|b$, then $ac|bc$. (vi) If $a|b$ and $a|c$, then $a|bx + cy$ for all $x, y \in \mathbb{Z}$.

(i) $1.a = a$. (ii) We have $b = am$, $a = bn$ for some m, n. If $b = 0$, then $a = 0$ and we are done. Thus it can be supposed that $b \neq 0$. By substitution, $b = am = bnm$ and cancelling b gives $1 = mn$. The only divisors of 1 are ± 1. Hence either $a = b$ or $a = -b$. (iii) We have $b = am$, $c = bn$. By substitution, $c = bn = a(mn)$. (iv) We have $bc = acm$. Since $c \neq 0$ it can be cancelled. (v) We have $a = bm$. Hence $ac = bcm$. (vi) We have $b = am$, $c = an$. Therefore $bx + cy = amx + any = a(mx + ny)$.

2. Prove that if n is odd, then $8|n^2 - 1$.

Since n is odd, it is of the form $2k-1$. Hence $n^2-1 = (2k-1)^2-1 = 4k^2-4k = 4k(k-1)$. If k is even, then $8|4k$. If k is odd, then $k - 1$ is even, so $8|4(k - 1)$.

3. (i) Show that if m and n are integers of the form $4k + 1$, then so is mn. (ii) Show that if $m, n \in \mathbb{N}$, and mn is of the form $4k - 1$, then so is one of m and n. (iii) Show that every number of the form $4k - 1$ has a prime factor of this form. (iv) Show that there are infinitely many primes of the form $4k - 1$.

(i) We have $(4k + 1)(4l + 1) = 16kl + 4k + 4l + 1 = 4(4kl + k + l) + 1$. (ii) m, n must be odd so are of the form $4k \pm 1$. If both are of the form $4k + 1$, then by (i) their product cannot be of the form $4k-1$. (iii) All the prime factors of $4k-1$ are odd, and so of the form $4k \pm 1$. If they were all of the form $4k + 1$, then by repeated use of (i), as in (ii), it would follow that their product is of wrong form. Hence at least one of them must be of the form $4k - 1$. (iv) Suppose that there are only a finite number of primes of the form $4k - 1$, say $p_1, p_2, \ldots, p_r$. Let $n = 4p_1 \ldots p_r - 1$. Obviously $n > 1$ and so by (iii) will have at least one prime factor p of the form $4k - 1$. But then $p|p_1 \ldots p_r$. Hence $p|4p_1 \ldots p_r - n = 1$ which is impossible.

4. Find all solutions x, $y \in \mathbb{Z}$ to the equation $x^2 - y^2 = 105$.

There are sixteen solutions given by the ordered pairs (x, y); $(\pm 53, \pm 52)$, $(\pm 19, \pm 16)$, $(\pm 13, \pm 8)$, $(\pm 11, \pm 4)$. One systematic way to see this is to write $d = x - y$, $s = x + y$, so that $ds = x^2 - y^2 = 105$. Solving for x and y gives $x = \frac{1}{2}(s + d)$, $y = \frac{1}{2}(s - d)$, and since s and d are both odd this gives a bijection between the solution set and the integer divisors of 105. Moreover interchanging s and d keeps x fixed and replaces y by $-y$, and replacing s and d by $-s$ and $-d$ changes the sign of both x and y. Thus it suffices to check the cases with $s > d > 0$, i.e (s, d) one of the four ordered pairs $(105, 1)$, $(35, 3)$, $(21, 5)$, $(15, 7)$.

5. Show that if $ad - bc = \pm 1$, then $(a + b, c + d) = 1$.

We have $(a + b, c + d)|(a + b)d - (c + d)b = ad - bc = \pm 1$.