

Math 465 Number Theory, Spring 2009, Practise Final, Solutions

1. Find $(1745, 1485)$ and integers x and y such that $1745x + 1485y = (1745, 1485)$.
 $(1745, 1485) = 5$, $x = 40$, $y = -47$.

2. Let x and y be integers which are not both 0. Suppose that $d \in \mathbb{N}$ is such that $d|x$, $d|y$ and, whenever $m \in \mathbb{N}$ and $m|x$ and $m|y$, one has $m|d$. (i) Prove that d is unique. This is the greatest common divisor (x, y) . (ii) Prove that if u and v are integers which are not both 0, then $(u, v) = (u, u + v)$. (i) Suppose d_1 and d_2 each have the necessary properties. Then $d_1 > 0$, $d_2 > 0$, $d_1|x$, $d_1|y$, $d_2|x$, $d_2|y$. Hence $d_2|d_1$ and $d_1|d_2$. Thus there are $k, l \in \mathbb{N}$ such that $d_1 = kd_2$ and $d_2 = ld_1$, and so $d_1 = kld_1$, $kl = 1$, $k = l = 1$. (ii) Let $d = (u, u + v)$. We have $(u, v)|u$ and $(u, v)|v$, so $(u, v)|u$ and $(u, v)|u + v$. Thus $(u, v)|d$. Also, $d|u$ and $d|u + v$. Hence $d|(u + v) - u = v$, so $d|u$ and $d|v$. Thus $d|(u, v)|d$ and hence $d = (u, v)$.

3. Solve the simultaneous congruences $x \equiv 3 \pmod{4}$, $x \equiv 2 \pmod{7}$, $x \equiv 7 \pmod{9}$. By Chinese remainder theorem, $x \equiv 3a7.9 + 2b4.9 + 7c4.7 \pmod{4.7.9}$ where $a7.9 \equiv 1 \pmod{4}$, $b4.9 \equiv 1 \pmod{7}$ and $c4.7 \equiv 1 \pmod{9}$. Thus we can take $a = 3$, $b = 1$, $c = 1$ and obtain $x \equiv 835 \equiv 79 \pmod{252}$.

4. Find all solutions to the congruence $9x^{58} + 4x^{30} + 2x \equiv 0 \pmod{29}$. By Fermat's little theorem the congruence reduces to $13x^2 + 2x \equiv 0 \pmod{29}$. Thus $x \equiv 0 \pmod{29}$ or $13x + 2 \equiv 0 \pmod{29}$, and so $x \equiv 0$ or $11 \pmod{29}$.

5. (i) Solve $f(x) = x^3 - x - 1 \equiv 0 \pmod{5}$. (ii) Use the Hensel-Newton method to find all solutions to $f(x) \equiv 0 \pmod{5^2}$. (i) Trying $x \equiv 0, 1, 2, 3, 4$ successively shows that only $x \equiv 2 \pmod{5}$ is a solution. (ii) $x_0 = 2$, $f(2) = 5$ and $f'(x) = 3x^2 - 1$, so $f'(2) = 11 \equiv 1 \pmod{5}$. Thus $f'(2)^{-1} \equiv 1 \pmod{5}$ and $x_1 = x_0 - f(x_0)/f'(x_0) \equiv 2 - 5 = -3 \equiv 22 \pmod{5^2}$.

6. Show that 3 is a primitive root modulo 17 and draw up a table of indices to this base. Hence, or otherwise, find all solutions to the following congruences. (i) $x^{16} \equiv 3 \pmod{17}$, (ii) $x^{21} \equiv 3 \pmod{17}$, (iii) $x^{30} \equiv 8 \pmod{17}$.

y	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	$\pmod{16}$
3^y	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1	$\pmod{17}$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	$\pmod{17}$
$\text{ind}_3 x$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8	$\pmod{16}$

(i) This is equivalent to $16y \equiv 1 \pmod{16}$ and is insoluble. (ii) This is equivalent to $21y \equiv 1 \pmod{16}$ and thus $y \equiv 13 \pmod{16}$ and so $x \equiv 12 \pmod{17}$. (iii) This is equivalent to $30y \equiv 10 \pmod{16}$, so $3y \equiv 1 \pmod{8}$ with $1 \leq y \leq 16$. Thus $y \equiv 3$ or $11 \pmod{16}$. Hence $x \equiv 10$ or $7 \pmod{17}$.

7. Evaluate the following Legendre symbols, showing your working. (i) $\left(\frac{-1}{103}\right)_L$, (ii) $\left(\frac{2}{103}\right)_L$, (iii) $\left(\frac{7}{103}\right)_L$, (iv) $\left(\frac{83}{103}\right)_L$. (i) $103 \equiv 3 \pmod{4}$, so $\left(\frac{-1}{103}\right)_L = -1$. (ii) $103 \equiv 7 \pmod{8}$, so $\left(\frac{2}{103}\right)_L = 1$. (iii) By law of quad. rec., $\left(\frac{7}{103}\right)_L = -\left(\frac{103}{7}\right)_L = -\left(\frac{5}{7}\right)_L = 1$. (iv) By law of quad. rec., $\left(\frac{83}{103}\right)_L = -\left(\frac{103}{83}\right)_L = -\left(\frac{20}{83}\right)_L = -\left(\frac{5}{83}\right)_L = -\left(\frac{83}{5}\right)_L = -\left(\frac{3}{5}\right)_L = 1$.

8. Find all solutions to the diophantine equation $x^2 + y^2 = 3z^2 + 3t^2$. If $x^2 + y^2 > 0$, then by Theorem 6.2, the left hand side is divisible exactly by 3 to an even power, but the right hand side is divisible exactly by 3 to an odd power. Hence $x^2 + y^2 = 0$ and so $x = y = z = t = 0$ is the only solution.