Math 465 Spring 2025 Practise Final Solutions
Note: The Final Exam for Math 465 will be Monday 5th May, 4:40pm to 6:30pm in room 312 Boucke.

1. Prove that if l, m and n are non-zero integers with $\mathrm{GCD}(l, m) = 1$ and $l|mn$, then $l|n$.

By definition of GCD there are x and y so that $lx + my = 1$, Since $l|mn$ we have $l|mnx + lyn = n(mx + ly) = n$.

2. Find $(1745, 1485)$ and integers x and y such that $1745x + 1485y = (1745, 1485)$.

$x_{-1} = 1$, $y_{-1} = 0$, $x_0 = 0$, $y_0 = 1$ $(1745, 1485) = 5$, $x = 40$, $y = -47$.

$1745 = 1 \times 1485 + 260$	$1 - 1 \times 0 = 1$	$0 - 1 \times 1 = -1$
$1485 = 260 \times 5 + 185$	$0 - 5 \times 1 = -5$	$1 - 5 \times (-1) = 6$
$260 = 1 \times 185 + 75$	$1 - 1 \times (-5) = 6$	$-1 - 1 \times 6 = -7$
$185 = 2 \times 75 + 35$	$-5 - 2 \times 6 = -17$	$6 - 2 \times (-7) = 20$
$75 = 2 \times 35 + 5$	$6 - 2 \times (-17) = 40$	$-7 = 2 \times 20 = -47$
$35 = 7 \times 5 + 0$.		

3. Solve the simultaneous congruences $x \equiv 3 \pmod 4$, $x \equiv 2 \pmod 7$, $x \equiv 7 \pmod 9$

By the Chinese remainder theorem, $x \equiv 7 \times 9 \times N_1 + 4 \times 9 \times N_2 + 4 \times 7 \times N_3 \pmod{4 \times 7 \times 9}$ where $7 \times 9 \times N_1 \equiv 3 \pmod 4$, $4 \times 9 \times N_2 \equiv 2 \pmod 7$, $4 \times 7 \times N_3 \equiv 7 \pmod 9$. Thus we can take $N_1 = 1$, $N_2 = 2$, $N_3 = 7$ and obtain $x \equiv 331 \equiv 79 \pmod{252}$.

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. Find a primitive root modulo 17 and draw up a table of discrete logarithms 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) $x^{30} \equiv 8 \pmod{17}$.

3 is a primitive root and

y	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^y	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{ord}_3 x$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

(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 $7 \pmod{17}$.

6. 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 quadratic reciprocity, $\left(\frac{7}{103}\right)_L = -\left(\frac{103}{7}\right)_L = -\left(\frac{5}{7}\right)_L = -\left(\frac{7}{5}\right)_L = -\left(\frac{2}{5}\right)_L = 1$. (iv) By law of quadratic reciprocity, $\left(\frac{83}{103}\right)_L = -\left(\frac{103}{83}\right)_L = -\left(\frac{20}{83}\right)_L = -\left(\frac{5}{83}\right)_L = -\left(\frac{83}{5}\right)_L = -\left(\frac{3}{5}\right)_L = 1$.

7. (i) Prove that -6 is a quadratic non-residue modulo 13 (ii) Prove that if $2x^2+3y^2 \neq 0$ and $13|2x^2+3y^2$, then 13 divides $2x^2+3y^2$ exactly to an even power. (iii) Find all solutions to the diophantine equation $2x^2 + 3y^2 = 26z^2 + 39t^2$.

(i) $\left(\frac{-6}{13}\right)_L = \left(\frac{7}{13}\right)_L = \left(\frac{13}{7}\right)_L = \left(\frac{-1}{7}\right)_L = -1$. (ii) If $13 \nmid y$, then $6x^2+(3y)^2 \equiv 0 \pmod{13}$ so $-6x^2$, and hence -6 would be a quadratic reside. Thus $13|y$ and thus $13|x$. If 13 were to divide $2x^2+3y^2$ exactly to an odd power, say 13^{2k+1}, then by repeated application of the above we would have $13^k|x$ and $13^k|y$, and 13 would divide $2(x/13^k)^2+3(y/13^k)^2$ exactly giving a contradiction. (iii) If $2x^2+3y^2 \neq 0$, then the LHS has to be divisible exactly be an even power of 13 whilst the RHS$= 13(2z^2+3t^2$ has to be divisible exactly by an odd power of 13, Hence the only solution is $x = y = z = t = 0$.

8. Let $\sigma(n)$ denote the sum of the divisors of n, $\sigma(n) = \sum_{m|n} m$. (i) When $X \geq 1$, prove that $\sum_{n \leq X} \frac{\sigma(n)}{n} = \sum_{m \leq X} \sum_{l \leq X/m} \frac{1}{l}$. (ii) Prove that $\sum_{n \leq X} \frac{\sigma(n)}{n} = \sum_{l \leq X} \frac{1}{l} \left\lfloor \frac{X}{l} \right\rfloor$. (iii) Prove that $\sum_{n \leq X} \frac{\sigma(n)}{n} = CX + O(\log X)$ where $C = \sum_{l=1}^{\infty} \frac{1}{l^2}$.

(i) The sum on the left is $\sum_{n \leq X} n^{-1} \sum_{m|n} m = \sum_{m \leq X} \sum_{n \leq X, m|n} m/n$ $= \sum_{m \leq X} \sum_{l \leq X/m} 1/l$ on interchanging the order of and substituting $n = lm$. (ii) Interchange the order of summation in the double sum in (i). $\sum_{l \leq X} \frac{1}{l} \sum_{m \leq X/l} 1 = \sum_{l \leq X} \frac{1}{l} \left\lfloor \frac{X}{l} \right\rfloor$. (iii) We can replace $\lfloor X/l \rfloor$ in (ii) by X/l with an error ≤ 1 for each term. Thus $\sum_{n \leq X} \frac{\sigma(n)}{n} = X \sum_{l \leq X} \frac{1}{l^2} + O(\log X)$. The sum in the main term differs from the infinite series by an amount not exceeding $\sum_{l > X} \frac{1}{l^2} \leq \frac{1}{X^2} + \int_X^{\infty} \frac{dt}{t^2}$ by monotonicity, and this is $= O(1/X)$.