PMATH 340 Number Theory, Solutions to Assignment 1

1: (a) Solve the Linear Diophantine Equation $385x - 1183y = 294$.

Solution: The Euclidean Algorithm gives

$$1183 = 3 \cdot 385 + 28\ ,\quad 385 = 13 \cdot 28 + 21\ ,\quad 28 = 1 \cdot 21 + 7\ ,\quad 21 = 3 \cdot 7 + 0$$

and so $\gcd(385, 1183) = 7$. Back Substitution gives the sequence

$$1\ ,\quad -1\ ,\quad 14\ ,\quad -43$$

and so we have $385(-43) + 1183(14) = 7$. Note that $\frac{294}{7} = 42$, and multiplying both sides by 42 gives $385(-1806) - 1183(-588) = 294$. Thus one solution is $(x, y) = (-1806, -588)$. Note that $\frac{385}{7} = 55$ and $\frac{1183}{7} = 169$, and so by the Linear Diophantine Equation Theorem, the general solution is

$$(x, y) = (-1806, -588) + k(169, 55)\ ,\ k \in \mathbb{Z}\,.$$

(b) A shopper spends \$19.81 to buy some bananas which cost 35 cents each and some plums which cost 56 cents each. What is the minimum number of pieces of fruit that the shopper could have bought.

Solution: Let x be the number of bananas purchased and let y be the number of plums purchased. The fruit is worth \$19.81, so we have

$$35x + 56y = 1981\,.$$

The Euclidean Algorithm gives

$$56 = 1 \cdot 35 + 21\ ,\quad 35 = 1 \cdot 21 + 14\ ,\quad 21 = 1 \cdot 14 + 7\ ,\quad 14 = 2 \cdot 7 + 0$$

so we have $\gcd(35, 56) = 7$. Back-Substitution gives

$$1\ ,\quad -1\ ,\quad 2\ ,\quad -3$$

so we have $35(-3) + 56(2) = 7$. Note that $\frac{1981}{7} = 283$ and multiplying both sides of the equation by 93 gives $35(-849) + 56(566) = 1981$, and so one solution is $(x, y) = (-849, 566)$. Note that $\frac{35}{7} = 5$ and $\frac{56}{7} = 8$, and so by the Linear Diophantine Equation Theorem, the general solution is

$$(x, y) = (-849, 566) + k(-8, 5)\ ,\ k \in \mathbb{Z}\,.$$

Note that

$$x \geq 0 \Longrightarrow -849 - 8k \geq 0 \Longrightarrow 8k \leq -849 \Longrightarrow k \leq \left\lfloor -\tfrac{849}{8} \right\rfloor = -107$$

$$y \geq 0 \Longrightarrow 566 + 5k \geq 0 \Longrightarrow 5k \geq -566 \Longrightarrow k \geq \left\lceil -\frac{566}{5} \right\rceil = -113\,,$$

so we obtain non-negative solutions when $-107 \leq k \leq 113$. We wish to choose the value of k which minimizes $x + y$ (the total number of pieces of fruit purchased). Note that

$$x + y = -849 - 8k + 566 + 5k = -283 - 3k\,,$$

so to minimize $x + y$ we must choose the maximum possible value of k, that is $k = -107$. When $k = -107$ we have $x + y = -283 - 3k = 38$. Thus the minimum number of pieces of fruit is 38.

2: We can solve a pair of linear diophantine equations in three variables by first eliminating one of the variables and solving the resulting equation in the remaining two variables.

(a) Show that there is no solution to the pair of diophantine equations

$$2x + 7y + \ z = 45 \qquad (1)$$
$$3x + 8y + 4z = 21 \qquad (2)$$

Solution: To eliminate z, multiply the first equation by 4 and subtract the second to get $5x + 20y = 159$. Notice that $\gcd(5, 20) = 5$ and 5 does not divide 159, so there is no solution.

(b) Find all solutions to the pair of diophantine equations

$$20x + 12y + 15z = 85 \qquad (1)$$
$$18x + 20y + \ 8z = 110 \qquad (2)$$

Solution: To eliminate z, multiply (2) by 15 and subtract 8 times (1). This gives

$$110x + 204y = 970 \qquad (3)$$

The Euclidean Algorithm gives

$$205 = 1 \cdot 110 + 94\ , \quad 110 = 1 \cdot 94 + 16\ , \quad 94 = 5 \cdot 16 + 14\ , \quad 16 = 1 \cdot 14 + 2\ , \quad 14 = 7 \cdot 2 + 0$$

so we have $\gcd(110, 204) = 2$. Back-Substitution gives

$$1\ , \quad -1\ , \quad 6\ , \quad -7\ , \quad 13$$

so we have $110(13) + 204(-7) = 2$. Note that $\frac{970}{2} = 485$, and multiplying both sides of the previous equation by 485 gives $110(6305) + 204(-3395) = 970$, and so one solution to (3) is given by $(x, y) = (6305, -3395)$. Note that $\frac{110}{2} = 55$ and $\frac{204}{2} = 102$, and so by the Linear Diophantine Equation Theorem, the general solution to equation (3) is

$$(x, y) = (6305, -3395) + k(-102, 55)\ ,\ k \in \mathbb{Z}\,.$$

Notice that taking $k = 62$ gives the solution $(x, y) = (-19, 15)$, so the general solution to (3) is also given by

$$(x, y) = (-19, 15) + k(-102, 55)\ ,\ k \in \mathbb{Z}\,.$$

Put $x = -19 - 102k$ and $y = 15 + 55k$ into (1) to get

$$20(-19 - 102k) + 12(15 + 55k) + 15z = 85$$

that is

$$-1380k + 15z = 285 \qquad (4)$$

Note that $1380 = 92 \cdot 15$ so that $\gcd(1380, 15) = 15$, and we have $285 = 19 \cdot 15$. By inspection, one solution to (4) is given by $(k, z) = (0, 19)$, and the general solution is

$$(k, z) = (0, 19) + \ell\,(1, 92)\ ,\ \ell \in \mathbb{Z}\,.$$

The complete solution to the pair of equations (1) and (2) is given by

$$x = -19 - 102\,k = -19 - 102\,\ell$$
$$y = 15 + 55\,k = 15 + 55\,\ell$$
$$z = 19 + 92\,\ell$$

or equivalently

$$(x, y, z) = (-19, 15, 19) + \ell\,(-102, 55, 92)\ ,\ l \in \mathbb{Z}\,.$$

3: (a) Find the prime factorization of $n = 2^{36} - 1$.

Solution: Recall that $a^2 - b^2 = (a-b)(a+b)$, $a^3 - b^3 = (a-b)(a^2+ab+b^2)$ and $a^3 + b^3 = (a+b)(a^2-ab+b^2)$. Use these rules repeatedly to get

$$\begin{aligned} 2^{36} - 1 &= (2^{18} - 1)(2^{18} + 1) \\ &= (2^9 - 1)(2^9 + 1)(2^6 + 1)(2^{12} - 2^6 + 1) \\ &= (2^3 - 1)(2^6 + 2^3 + 1)(2^3 + 1)(2^6 - 2^3 + 1)(2^2 + 1)(2^4 - 2^2 + 1)(2^{12} - 2^6 + 1) \\ &= 7 \cdot 73 \cdot 9 \cdot 57 \cdot 5 \cdot 13 \cdot 4033 \\ &= 7 \cdot 73 \cdot 3^2 \cdot 3 \cdot 19 \cdot 5 \cdot 13 \cdot 4033 \,. \end{aligned}$$

Note that 73 is prime, since $\lfloor \sqrt{73} \rfloor = 8$, and none of the primes 2, 3, 5, 7 is a factor of 73. To determine whether 4033 is prime, we test every prime p with $p \leq \lfloor \sqrt{4033} \rfloor = 63$ to see if it is a factor. Using the Sieve of Eratosthenes, we find that the primes we need to check are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61 \,,$$

and when we test these we find that 37 is a factor, indeed $4033 = 37 \cdot 109$. Note that 109 is prime, since $\lfloor \sqrt{109} \rfloor = 10$ and none of the primes 2, 3, 5, 7 is a factor of 109. Thus we obtain the prime factorization

$$2^{36} - 1 = 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 109 \,.$$

(b) Find the exponent of 3 in the prime factorization of $\binom{100}{40} = \frac{(100)!}{(40)!(60)!}$.

Solution: Recall that $e(p, m)$ denotes the exponent of p in the prime factorization of m. We have

$$\begin{aligned} e(3, 100!) &= \left\lfloor \tfrac{100}{3} \right\rfloor + \left\lfloor \tfrac{100}{9} \right\rfloor + \left\lfloor \tfrac{100}{27} \right\rfloor + \left\lfloor \tfrac{100}{81} \right\rfloor = 33 + 11 + 3 + 1 = 48 \\ e(3, 60!) &= \left\lfloor \tfrac{60}{3} \right\rfloor + \left\lfloor \tfrac{60}{9} \right\rfloor + \left\lfloor \tfrac{60}{27} \right\rfloor = 20 + 6 + 2 = 28 \\ e(3, 40!) &= \left\lfloor \tfrac{40}{3} \right\rfloor + \left\lfloor \tfrac{40}{9} \right\rfloor + \left\lfloor \tfrac{40}{27} \right\rfloor = 13 + 4 + 1 = 18 \end{aligned}$$

and so $e\left(3, \binom{60}{40}\right) = e(3, 100!) - e(3, 60!) - e(3, 40!) = 48 - 28 - 18 = 2$.

(c) Let $a = \prod_{k=1}^{6} k^k$. Find the number of factors (positive or negative) of a which are either perfect squares or perfect cubes (or both).

Solution: Let us find the prime factorization of a. We have

$$\begin{aligned} a = \prod_{k=1}^{6} k^k &= 1^1 \cdot 2^2 \cdot 3^3 \cdot 4^4 \cdot 5^5 \cdot 6^6 \\ &= 2^2 \cdot 3^3 \cdot 2^8 \cdot 5^5 \cdot 2^6 \cdot 3^6 \\ &= 2^{16} \cdot 3^9 \cdot 5^5 \,. \end{aligned}$$

The positive factors of a are of the form $2^i \cdot 3^j \cdot 5^k$ with $0 \leq i \leq 16$, $0 \leq j \leq 9$, and $0 \leq k \leq 5$. The factors of a which are perfect squares are of the form $2^i \cdot 3^j \cdot 5^k$ with $i = 0, 2, 4, \cdots, 16$, $j = 0, 2, 4, 6, 8$, and $k = 0, 2, 4$. There are 9 choices for i, 5 for j, and 3 for k, so the number of square factors is equal to $9 \cdot 5 \cdot 3 = 135$. The factors of a which are perfect cubes are of the form $\pm 2^i \cdot 3^j \cdot 5^k$ with $i = 0, 3, 6, 9, 12, 15$, $j = 0, 3, 6, 9$ and $k = 0, 3$. There are 6 choices for i, 4 for j, and 2 for k, so there are $6 \cdot 4 \cdot 2 = 48$ positive cube factors and another 48 negative cube factors. Finally, note that some of the 48 positive cube factors are also squares, indeed the sixth powers are both cubes and squares. The sixth powers are of the form $2^i \cdot 3^j \cdot 5^k$ with $i = 0, 6, 12$, $j = 0, 6$ and $k = 0$, so there are $3 \cdot 2 \cdot 1 = 6$ sixth powers. Thus the total number of factors (positive or negative) which are squares or cubes is $135 + 48 + 48 - 6 = 225$.

4: (a) Prove that for all positive integers a and b, we have $a|b$ if and only if $a^2|b^2$.

Solution: Write $a = {p_1}^{j_1}{p_2}^{j_2}\cdots{p_n}^{j_n}$ and $b = {p_1}^{k_1}{p_2}^{k_2}\cdots{p_n}^{k_n}$ where the p_i are distinct primes. Then we have $a^2 = {p_1}^{2j_1}{p_2}^{2j_2}\cdots{p_n}^{2j_n}$ and $b^2 = {p_1}^{2k_1}{p_2}^{2k_2}\cdots{p_n}^{2k_n}$, and so

$$a|b \iff j_i \le k_i \text{ for all } i \iff 2j_i \le 2k_i \text{ for all i} \iff a^2|b^2\,.$$

(b) Prove that for all positive integers a, b and c, if $c|ab$ then $c|\gcd(a,c)\gcd(b,c)$.

Solution: Write $a = {p_1}^{j_1}{p_2}^{j_2}\cdots{p_n}^{j_n}$, $b = {p_1}^{k_1}{p_2}^{k_2}\cdots{p_n}^{k_n}$ and $c = {p_1}^{m_1}{p_2}^{m_2}\cdots{p_n}^{m_n}$. Note that

$$\begin{aligned} ab &= {p_1}^{j_1+k_1}{p_2}^{j_2+k_2}\cdots{p_n}^{j_n+k_n} \\ \gcd(a,c) &= {p_1}^{\min\{j_1,m_1\}}{p_2}^{\min\{j_2,m_2\}}\cdots{p_n}^{\min\{j_n,m_n\}} \\ \gcd(b,c) &= {p_1}^{\min\{k_1,m_1\}}{p_2}^{\min\{k_2,m_2\}}\cdots{p_n}^{\min\{k_n,m_n\}} \\ \gcd(a,c)\gcd(b,c) &= {p_1}^{\min\{j_1,m_1\}+\min\{k_1,m_1\}}{p_2}^{\min\{j_2,m_2\}+\min\{k_2,m_2\}}\cdots{p_n}^{\min\{j_n,m_n\}+\min\{k_n,m_n\}}\,. \end{aligned}$$

Suppose that $c|ab$ so we have $m_i \le j_i + k_i$ for all i. Fix an index i. We consider three cases.

Case 1. If $m_i \le j_i$ then we have $m_i = \min\{j_i, m_i\} \le \min\{j_i, m_i\} + \min\{k_i, m_i\}$.

Case 2. If $m_i \le k_i$ then we have $m_i = \min\{k_i, m_i\} \le \min\{j_i, m_i\} + \min\{k_i, m_i\}$.

Case 3. If $m_i \ge j_i$ and $m_i \ge k_i$ then we have $m_i \le j_i + k_i = \min\{j_i, m_i\} + \min\{k_i, m_i\}$.

In all three cases we have $m_i \le \min\{j_i, m_i\} + \min\{k_i, m_i\}$. Thus $c|\gcd(a,c)\gcd(b,c)$ as required.

(c) Prove that for all integers a, b and c, we have $\gcd(ac, bc) = c\gcd(a,b)$.

Solution: Let $d = \gcd(a,b)$ and let $e = \gcd(ac,bc)$. We must show that $e = dc$. Since $c|ac$ and $c|bc$ we have $c|e$ (by Theorem 1.10), say $e = kc$. Since $e|ac$, so $kc|ac$, we have $k|a$, and since $e|bc$, so $kc|bc$, we have $k|b$, and so k is a common divisor of a and b. Since d is the greatest common divisor of a and b, we must have $k \le d$, and hence $kc \le dc$, that is $e \le dc$. On the other hand, we have $d|a$ so $dc|ac$, and we have $d|b$ so $dc|bc$, and so dc is a common divisor of ac and bc. Since e is the greatest common divisor of ac and bc, we must have $dc \le e$. We have shown that $e \le dc$ and that $dc \le e$, so we have $e = dc$, as required.

(d) Prove that for all positive integers a and b, we have $\gcd(a,b) = \gcd\big(a+b, \operatorname{lcm}(a,b)\big)$.

Solution: Let $d = \gcd(a,b)$, $m = \operatorname{lcm}(a,b)$, and $e = \gcd(a+b, m)$. We must show that $d = e$. Write $a = dk$ and $b = d\ell$ so we have $\gcd(k,\ell) = 1$ (by Theorem 1.10) and $m = dk\ell$ (by Theorem 1.28). By Part (c), we have

$$e = \gcd(a+b, m) = \gcd(d(k+\ell), dk\ell) = d\gcd(k+\ell, k\ell)\,,$$

so it suffices to show that $\gcd(k+\ell, k\ell) = 1$. Suppose, for a contradiction, that $\gcd(k+\ell, k\ell) \ne 1$. Let p be a common prime factor of $k+\ell$ and $k\ell$. Since p is prime and $p|k\ell$, we know that $p|k$ or $p|\ell$. If $p|k$ then since $p|(k+\ell)$ we also have $p|\ell$. Similarly, if $p|\ell$ then since $p|(k+\ell)$ we also have $p|k$. In either case we see that p is a common prime factor of k and ℓ, which contradicts the fact that $\gcd(k,\ell) = 1$.