M3P14 EXAMPLE SHEET 1 SOLUTIONS

1a. Express 14 as an integer linear combination of 280 and 203.
We have:

$$\begin{aligned} 280 &= 1(203) + 77 \\ 203 &= 2(77) + 49 \\ 77 &= 1(49) + 28 \\ 49 &= 1(28) + 21 \\ 28 &= 1(21) + 7 \end{aligned}$$

Therefore:

$$\begin{aligned} 7 &= 28 - 21 \\ &= 28 - (49 - 28) \\ &= 2(28) - 49 \\ &= 2(77 - 49) - 49 \\ &= 2(77) - 3(49) \\ &= 2(77) - 3(203 - 2(77)) \\ &= 8(77) - 3 * (203) \\ &= 8(280 - 203) - 3(203) \\ &= 8 * 280 - 11 * 203 \end{aligned}$$

We thus have $14 = 16 * 280 - 22 * 203$.
1b. Find, with proof, all solutions to the linear diophantine equation $10x + 25y = 45$.
Clearly one solution is $x = 2, y = 1$. If (x, y) is another solution, then $10(x-2)+25(y-1) = 0$. Dividing by 5 we get $2(x-2)+5(y-1) = 0$. Since $(2, 5) = 1$, we must then have $5|x - 2$; i.e. $x = 5k + 2$ for some k. Solving for y we find $y = -2k + 1$. Substituting into the original equation, we find that $(5k + 2, -2k + 1)$ is a solution for all k.
1c. Find a multiplicative inverse of 5 modulo 132.
We have $132 = 26(5) + 2$ and $5 = 2(2) + 1$. Thus $1 = 5 - 2(132 - 26(5)) = 53(5) - 2(132)$. Thus $53(5)$ is congruent to 1 mod 132, and 53 is the desired inverse.
1d. Find an integer congruent to 7 mod 25 and congruent to 1 mod 16.

We have $25 = 16+9$, $16 = 9+7$, $9 = 7+2$, $7 = 3(2)+1$. Thus $1 = 7-3(2) = 3(9)-4(7) = 4(16)-7(9) = 11(16)-7(25)$. Thus $7(11(16))-7(25) = 1057$ is congruent to 7 mod 25 and congruent to 1 mod 16.

1e. Find, with proof, the smallest nonnegative integer n such that $n \equiv 1 \pmod 3$, $n \equiv 2 \pmod 5$, and $n \equiv 3 \pmod 7$.

We have $1 = 2(3)-5$, so $2(2(3))-5 = 7$ is congruent to 1 mod 3 and 2 mod 5. We thus know that $n \equiv 7 \pmod{15}$ by the uniqueness in the Chinese Remainder Theorem. We have $1 = 15-2(7)$, so $3(15)-7(2(7)) = -53$ is congruent to 7 (mod 15) and 3 (mod 7). Thus n is congruent to -53 (mod 105) by the Chinese remainder theorem. Since 52 is the smallest positive integer congruent to -53 mod 105, we must have $n = 52$.

2. Least Common Multiples

2a. Let a and b be nonzero integers. Show that there is a unique positive integer m with the following two properties:

- a and b divide m, and
- If n is any number divisible by both a and b, then $m|n$.

The number m is called the *least common multiple* of a and b.

We first show that m is unique. Let n be another positive integer with the same properties. Then a and b divide n by the first property (of n), so by the second property (of m) we have $m|n$. Similarly, by the first property (of m) and the second property (of n) we have $n|m$. So $m = \pm n$, but both are positive, so $m = n$.

Existence of m will follow from part 2b, below:

2b. Show that the least common multiple of a and b is given by $\frac{|ab|}{(a,b)}$.

It is clear that $\frac{|ab}{(a,b)}$ is positive. It is divisible by a because $\frac{b}{(a,b)}$ is an integer, and similarly is divisible by b. We must thus show that if a and b divide n, then so does $\frac{|ab|}{(a,b)}$. But a and $\frac{b}{(a,b)}$ are relatively prime, and both divide n, so their product does as well.

3. Show that the equation $ax \equiv b \pmod n$ has no solutions if b is not divisible by (a,n), and exactly (a,n) solutions in $\mathbb{Z}/n$ otherwise.

If $ax \equiv b \pmod n$, then $ax - b = kn$ for some integer k. Since both ax and kn are divisible by (a,n), b must be as well.

Suppose that b is divisible by (a,n). Then solving $ax - b = kn$ is the same as solving $cx - d = km$, where $c = \frac{a}{(a,n)}$, $d = \frac{b}{(a,n)}$, $m = \frac{n}{(a,n)}$. Since c and m are relatively prime, this equation has a unique solution y modulo m. Thus any x that is congruent to y modulo m is a solution. Since there are (a,n) congruence clases modulo n that are congruent to a given congruence class mod m, we are done.

4. Let p be a prime, and a be any integer. Show that a^{p^2} is congruent to a modulo p.

Note that if p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$, so $a^p \equiv a \pmod{p}$. If p does divide a, then a and a^p are both $0 \pmod{p}$. Thus $a^p \equiv a \pmod{p}$ for *all* a. Now $a^{p^2} = (a^p)^p \equiv a^p \equiv a \pmod{p}$.

5. Let n be a squarefree positive integer, and suppose that for all primes p dividing n, we have $(p-1)|(n-1)$. Show that for all integers a with $(a,n) = 1$, we have $a^n \equiv a \pmod{n}$.
Since n is squarefree, it is the product of the primes that divide it. Therefore, by the uniqueness part of the Chinese remainder theorem, it suffices to show that $a^n \equiv a \pmod{p}$ for all p dividing n. Since $(a,n) = 1$, p does not divide a, and so $a^{p-1} \equiv 1 \pmod{p}$. Since $(p-1)|(n-1)$, we have $n = 1 + k(p-1)$ for some k. Then $a^n = a(a^{p-1})^k \equiv a \pmod{p}$ as claimed.

6. Let n be a positive integer. Show that the sum $\sum_{d|n, d>0} \Phi(d)$ is equal to n.
For any positive integer a less than or equal to n, (a,n) is a positive divisor d of n. It follows (since n is the number of positive integers less than or equal to n) that we have:

$$n = \sum_{d|n, d>0} \#\{a : 1 \leq a \leq n, (a,n) = \frac{n}{d}\}.$$

Therefore, it suffices to show that the number of positive integers a between 1 and n with $(a,d) = \frac{n}{d}$ is $\Phi(d)$. But multiplication by $\frac{n}{d}$ gives a bijection between the set of positive integers b with $1 \leq b \leq d$ and $(b,d) = 1$, and the set of positive integers a with $1 \leq a \leq n$ and $(a,n) = \frac{n}{d}$. Thus these sets both have $\Phi(d)$ elements.
NOTE: this can also be done by induction on the number of primes dividing n.

7. (BONUS) Show that the sum $\sum_{p \text{ prime}, p>0} \frac{1}{p}$ diverges.
Suppose that this sum converges. Then there exists a prime q such that

$$\sum_{p \text{ prime}, p \geq q} \frac{1}{p} < \frac{1}{2}.$$

Call this sum S. Since $S < 1$, the geometric series $S + S^2 + S^3 + \ldots$ converges. We will show that this is impossible.
For each i, let T_i be the set of positive integers that are the product of precisely i (not necessarily distinct) primes p, each of which is greater than or equal to q.
Squaring the series for S, we find that:

$$S^2 = \sum_{n \in T_2} c_n \frac{1}{n} > \sum_{n \in T_2} \frac{1}{n},$$

where c_n is 1 or 2 (depending on whether n is a square of a prime or a product of two distinct primes.) Similarly, expanding out the ith power of the series for S, we find:

$$S^i > \sum_{n \in T_i} \frac{1}{n}.$$

The union T of the T_i is the set of all positive integers that are divisible only by primes greater than or equal to q. The sum $S + S^2 + S^3 + ...$ then satisfies:

$$S + S^2 + S^3 + ... > \sum_{n \in T} \frac{1}{n}.$$

Let Q be the product of all primes *less than* q. Then for any integer k, $Qk + 1$ is only divisible by primes greater than or equal to q; in particular $Qk + 1$ lies in T. Thus $\frac{1}{Qk+1}$ appears as a summand in $\sum_{n \in T} \frac{1}{n}$ for all k.

We must therefore have $S + S^2 + S^3 + ... > \sum_{k=1}^{\infty} \frac{1}{Qk+1}$. But the latter series diverges, so this is a contradiction.