Melbourne High School
Maths Extension Group 2023
Term 1 Week 9 Handout Solutions

§1. More combinatorics problems

§2. Euclid's Algorithm

1. Let $g = \gcd(a, b)$. First solve
$$ax - by = g$$
and then multiply the solution by n/g, for if (x', y') satisfies $ax' - by' = g$ then $(x'n/g, y'n/g)$ satisfies
$$\frac{ax'n}{g} - \frac{by'n}{g} = n.$$

2. $(x, y) = (5, 16)$.

3. We get a solution, but the solution is not in positive integers: $(x, y) = (-10, -23)$. To get the solution in positive integers, we argue generally. Suppose $x = x'$ and $y = y'$ are the solutions we have found that are both not positive integers. To make them positive integers, we need to add a number to both without changing the equality sign. We note that
$$7200(x' + M) - 3132(y' + N) = 36$$
if and only if $7200M = 3132N$. Cancelling 36 from both sides we get $200M = 87N$. Therefore we can take $M = 87$ and $N = 200$ (this is the 'smallest' solution because 200 and 87 are coprime).

   Our original solution was $x' = -10$ and $y' = -23$, so our positive integer solution is $(x, y) = (77, 177)$.

4. Let $u = u'$ and $v = v'$ be the integers satisfying the equation
$$ux + vy = \gcd(x, y).$$
Therefore we have
$$a^{\gcd(x,y)} \equiv a^{u'x+v'y} \equiv (a^x)^u (a^y)^v \equiv 1 \cdot 1 \equiv 1 \pmod{n}.$$

5. We want to show that the equations
$$N = am$$
and
$$N + k = bn$$
for integers m and n are soluble. Putting the first into the second we get
$$am + k = bn$$
which implies
$$am - bn = k.$$
This equation is always soluble because a and b are coprime.

6. Suppose that p does not divide a (if it did we have nothing to prove), Our goal now is to show that it divides b.

   If p does not divide a, then it must be coprime with a. Hence there exist positive integers x and y such that

   $$px - ay = 1.$$

   Multiplying both sides by b yields

   $$pbx - aby = b.$$

   Clearly p divides pbx, and by assumption p divides ab, so it must divide aby too. But if p divides both pbx and aby, it must divide their difference, which is b.