Handout: Proof skills

(1) Write the negation of each of the following statements.
   (a) The numbers a and b are in the set S.
   Either a or b is not in S.
   (b) Either a or b is in the set S.
   Neither of a or b is in the set S.
   (c) There exists a solution to the linear equivalence $10x \equiv 6 \mod (12)$.
   There is no solution to the linear equivalence $10x \equiv 6 \mod (12)$.
   (d) Every integer is even.
   There exists an odd integer.

(2) Let a, b, c, q be integers and p be a prime number. For each pair of statements x and y below, determine whether the statement "x and y" and the statement "x or y" are true or false.
   (a) x = "Every natural number can be factored uniquely into a product of primes."
   y = "If $a \mid b$ and $b \mid c$, then $a \mid c$."
   Both x and y are true, so "x and y" and "x or y" are both true.
   (b) x = "There are infinitely many primes of the form $12q + 7$."
   y = "If $\gcd(a, p^2) = p$, then $\gcd(a^2, p^2) = ap$."
   x is true, while y is false (consider $a = 6$, $p = 2$). So "x and y" is false and "x or y" is true.
   (c) x = "There are 5 distint congruence classes modulo 6."
   y = " If $a \mid b$ and $b \mid a$, then $a = b$."
   x is false (there are 6) and y is false (it could be that $a = -b$), so "x and y" and "x or y" are both false.

(3) Prove the following statement using a direct proof.

Theorem 1. *Let n, a, b, and c be positive integers. If $a \equiv_n b$ and $b \equiv_n c$, then $a \equiv_n c$.*

Proof. Suppose that n, a, b, and c be positive integers and $a \equiv_n b$ and $b \equiv_n c$. Then $n \mid (a-b)$ and $n \mid (b-c)$. In other words, $a - b = qn$ and $b - c = q'n$ for some integers q, q'. Therefore,

$$a - c = (a - b) + (b - c) = qn + q'n = (q + q')n$$

and we have that $n \mid (a - c)$. In other words, $a \equiv_n c$. □

(4) Prove the following statements using a proof by contradiction.

Theorem 2. *If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.*

Proof. Suppose, towards a contradiction, that $a, b \in \mathbb{Z}$ and $a^2 - 4b = 2$. Then $a^2 = 4b - 2 = 4(b-1) + 2$. In particular, a^2 has remainder 2 when divided by 4. We showed on Day 1 of the course that each perfect square has remainder 0 or 1 when divided by 4. So we have reached a contradiction. □

Theorem 3. *The number $\sqrt{2}$ is irrational.*

Proof. Suppose, towards a contradiction, that $\sqrt{2}$ is a rational number. Then it can be written as a fully reduced fraction $\sqrt{2} = \frac{a}{b}$. Squaring both sides and multiplying by b^2, we see that $2b^2 = a^2$. Therefore, a^2 is an even number. If $2|a^2$, then it follows that $2|a$ (since 2 is prime). Thus a is an even number and we can write $a = 2k$ for some integer k. Then $\sqrt{2} = \frac{2k}{b}$ and the same process shows that $2b^2 = (2k)^2 = 4k^2$. Dividing by two, we see that $b^2 = 2k^2$ and so b^2 is even. Again, this implies that b is even. This is a contradiction because the fraction $\frac{a}{b}$ was assumed to be fully reduced, but we have just shown that both the numerator and denominator are divisible by 2. So we conclude that $\sqrt{2}$ is irrational. □

(5) Prove the following statement by proving its contrapositive.

Theorem 4. *Let x and y be integers. If $x+y$ is even, then x and y are both even or x and y are both odd.*

Proof. Suppose that one of x and y is odd and the other is even. Say, $x = 2k$ and $y = 2k'+1$ for some $k, k' \in \mathbb{Z}$. Then $x+y = 2k+(2k'+1) = 2(k+k')+1$ and so $x+y$ is odd. This proves the contrapositive of the statement, thus the statement holds. □

(6) Prove the following "if and only if" statement.

Theorem 5. *Suppose that* $\gcd(a,n) = 1$ *and* $m \mid a$ *and* $m \mid b$. *Then*

$$ax \equiv b \mod (n) \quad \textit{iff} \quad \left(\frac{a}{m}\right) x \equiv \left(\frac{b}{m}\right) \mod (n).$$

Proof. $\boxed{\Rightarrow}$ Suppose that $\gcd(a,n) = 1$, $m \mid a$, $m \mid b$, and $ax \equiv b \mod (n)$. Then $n \mid (ax-b)$. In other words,

$$nq = ax - b$$

for some integer q. Dividing both sides by m, we get

$$\frac{nq}{m} = \frac{a}{m}x - \frac{b}{m}. \tag{1}$$

Since $m \mid a$ and $m \mid b$, we know that the right-hand side of this equation is an integer. This means that $\frac{nq}{m}$ is also an integer. Furthermore, since $\gcd(a,n) = 1$, we know that $m \mid a$ implies that $m \nmid n$ unless $m = 1$. So it must be that $\frac{q}{m}$ is an integer. Thus Equation (1) implies that $n \mid \left(\frac{a}{m}x - \frac{b}{m}\right)$ and so

$$\left(\frac{a}{m}\right) x \equiv \left(\frac{b}{m}\right) \mod (n),$$

as desired.

$\boxed{\Leftarrow}$ Suppose that $\gcd(a,n) = 1$, $m \mid a$, $m \mid b$, and $\left(\frac{a}{m}\right) x \equiv \left(\frac{b}{m}\right) \mod (n)$. Then $n \mid \left(\frac{a}{m}x - \frac{b}{m}\right)$ and we have that, for some $q \in \mathbb{Z}$,

$$nq = \frac{a}{m}x - \frac{b}{m}.$$

Multiplying through by m, we see that

$$nmq = ax - b$$

and so $n \mid (ax - b)$. Therefore, $ax \equiv b \mod (n)$, as desired. $\square$