MATH 521A: Abstract Algebra
Homework 2 Solutions

1. Find all primes between 1000 and 1050.

   There are eight: 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049.

2. Let $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ and $b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ where $p_1, \ldots, p_k$ are distinct positive prime integers, and each $r_i, s_i \in \mathbb{N}_0$. Prove that $a|b$ if and only if $\forall i \in [1,k], r_i \leq s_i$.

   $\rightarrow$: Suppose $a|b$. Then $\frac{b}{a} \in \mathbb{N}$. But $\frac{b}{a} = p_1^{s_1-r_1} p_2^{s_2-r_2} \cdots p_k^{s_k-r_k}$. If any exponent is negative, $\frac{b}{a}$ could not be an integer because the primes are all distinct, so that prime power in the denominator will not cancel with anything else. Hence each exponent is nonnegative, so $s_i \geq r_i$ for all $i \in [1,k]$.
   $\leftarrow$: Suppose $\forall i \in [1,k], r_i \leq s_i$. Then $c = p_1^{s_1-r_1} p_2^{s_2-r_2} \cdots p_k^{s_k-r_k}$ is an integer, and we calculate $ac = b$, so $a|b$.

3. Let $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ and $b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ where $p_1, \ldots, p_k$ are distinct positive prime integers, and each $r_i, s_i \in \mathbb{N}_0$. Determine, with proof, the prime factorization of $\gcd(a,b)$ and $\text{lcm}(a,b)$.

   Set $d = p_1^{\min(r_1,s_1)} p_2^{\min(r_2,s_2)} \cdots p_k^{\min(r_k,s_k)}$. Since $\min(r_i, s_i) \leq r_i$ and $\min(r_i, s_i) \leq s_i$, we apply Problem 2 and conclude that $d|a$ and $d|b$. Hence d is a common divisor of a, b. Suppose that c is some other common divisor, i.e. $c|a$ and $c|b$. By problem 2 again, we may write $c = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ with $t_i \leq r_i$ and $t_i \leq s_i$ for all i. Hence $t_i \leq \min(r_i, s_i)$, so by problem 2 a third time, $c|d$. Thus $d = \gcd(a,b)$ by Cor 1.3.

   Set $e = p_1^{\max(r_1,s_1)} p_2^{\max(r_2,s_2)} \cdots p_k^{\max(r_k,s_k)}$. Since $\max(r_i, s_i) \geq r_i$ and $\max(r_i, s_i) \geq s_i$, we apply Problem 2 and conclude that $a|e$ and $b|e$. Hence e is a common multiple of a, b. Suppose that c is some other common multiple, i.e. $a|c$ and $b|c$. By problem 2 again, we may write $c = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ with $t_i \geq r_i$ and $t_i \geq s_i$ for all i. Hence $t_i \geq \max(r_i, s_i)$, so by problem 2 a third time, $e|c$. Thus $d = \text{lcm}(a,b)$ by a theorem from class.

4. Let $a, b, m, n \in \mathbb{N}$. Prove that $a^m | b^m$ if and only if $a^n | b^n$.

   Let $\{p_1, p_2, \ldots p_k\}$ be the set of all (distinct) positive primes that divide a, b, or both. By the FTA (Thm. 1.8) we may write a, b as in problem 2. In particular, $a^m = p_1^{mr_1} p_2^{mr_2} \cdots p_k^{mr_k}$, with b^m, a^n, b^n similarly. Suppose that $a^m | b^m$. By problem 2, we conclude that for all i, $mr_i \leq ms_i$. Hence $r_i \leq s_i$, and also $nr_i \leq ns_i$. By problem 2 again, we conclude that $a^n | b^n$. The reverse direction is similar (suppose $a^n | b^n$, apply problem 2 to get $\forall i \; nr_i \leq ns_i$, use algebra to get $mr_i \leq ms_i$, apply problem 2 again to get $a^m | b^m$).

5. Prove that, for all $n \geq 2$, there are no primes among $\{n! + 2, n! + 3, \ldots, n! + n\}$.
   Since $n! = 1 \cdot 2 \cdots (n-1) \cdot n$, each integer in $[2, n]$ divides $n!$. Hence, for each $i \in [2, n]$, we have $n! + i = i(\frac{n!}{i} + 1)$. Each of i, $\frac{n!}{i} + 1$ is an integer greater than 1, so $n! + i$ can't be prime.

6. Prove that, for integer a, b and prime p:

   $$ab \equiv 0 \pmod{p} \text{ if and only if } [\ a \equiv 0 \pmod{p} \text{ or } b \equiv 0 \pmod{p}\ ]$$

   Now assume p is composite and disprove the statement.

   $\rightarrow$: Suppose that $ab \equiv 0 \pmod{p}$. Then $p|ab$. By Thm 1.5 (the "true" definition of primes), either $p|a$ or $p|b$. Hence either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.
   $\leftarrow$: Suppose that $[\ a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}\ ]$. If $a \equiv 0 \pmod{p}$, then $p|a$, so there is some integer c with $a = pc$. Then $ab = pcb$, so $p|ab$. If $b \equiv 0 \pmod{p}$, then $p|b$, so there is some intger d

with $b = pd$. Then $ab = pda$, so $p|ab$. Either way, $p|ab$, so $ab \equiv 0 \pmod{p}$.
Now, if p is composite, we may write $p = ab$ for some natural a, b. We have $p \nmid a$, since $a < p$ (proved in HW 1), and also $p \nmid b$. Thus $a \not\equiv 0 \pmod{p}$ and $b \not\equiv 0 \pmod{p}$, and yet $ab = p \equiv 0 \pmod{p}$.

7. Prove that, for integer a, b and prime p:

$$a^2 \equiv b^2 \pmod{p} \text{ if and only if } [\ a \equiv b \pmod{p} \text{ or } a \equiv -b \pmod{p}\ ]$$

Now find a composite p and a, b to disprove the statement.

We use Thm 2.2(1) to rewrite $a \equiv b$ as $(a - b) \equiv 0$. We rewrite $a \equiv -b$ as $(a + b) \equiv 0$. We rewrite $a^2 \equiv b^2$ as $a^2 - b^2 = (a - b)(a + b) \equiv 0$.

$\leftarrow$: This follows by Thm 2.2(2), whether or not p is prime. If either $(a + b) \equiv 0$ or $(a - b) \equiv 0$, then their product $(a + b)(a - b) \equiv 0$.

$\rightarrow$: We use Problem 6 (and now we need p to be prime). Since $(a - b)(a + b) \equiv 0 \pmod{p}$, we conclude that either $(a - b) \equiv 0$ or $(a + b) \equiv 0$.

Most composite p admit a counterexample (though not all, e.g. $n = 6$). For example, take $n = 8$, $a = 1, b = 3$. $a^2 \equiv 1 \equiv b^2 \pmod{8}$, yet $a \not\equiv b \pmod{8}$ and $a \not\equiv -b \pmod{8}$.

8. Let $a, b, c, n \in \mathbb{N}$. Prove that $a \equiv b \pmod{n}$ if and only if $ac \equiv bc \pmod{nc}$.

$\rightarrow$: Suppose that $a \equiv b \pmod{n}$. Hence $n|a - b$, and there is some m where $nm = (a - b)$. Multiplying both sides by c, we get $ncm = (a - b)c = (ac - bc)$. Hence $nc|(ac - bc)$, so $ac \equiv bc \pmod{nc}$.
$\leftarrow$: Suppose that $ac \equiv bc \pmod{nc}$. Hence $nc|(ac - bc)$, and there is some k where $nck = ac - bc = (a - b)c$. Dividing by the nonzero c gives $nk = a - b$. Hence $n|(a - b)$, so $a \equiv b \pmod{n}$.

9. Let $a, b, n \in \mathbb{N}$. Determine the exact conditions under which the modular equation

$$ax \equiv b \pmod{an}$$

has solutions (for x).

If $a|b$, then we apply Problem 8, and get a solution for x (unique mod n). If however, $a \nmid b$, we will prove that there is no solution. Suppose by way of contradiction there is. Then $an|(ax - b)$, so there is some integer c with $anc = ax - b$. We rewrite as $b = ax - anc = a(x - nc)$. Note that a divides the right hand side, but by assumption does not divide the left hand side; this is a contradiction. Hence the modular equation has a solution exactly when $a|b$.

10. Let $a, b, m, n \in \mathbb{N}$. Prove that:

$$[\ a \equiv b \pmod{m} \text{ and } a \equiv b \pmod{n}\ ] \text{ if and only if } a \equiv b \pmod{\operatorname{lcm}(m, n)}$$

$\rightarrow$: Since $a \equiv b \pmod{m}$, then $m|(a - b)$. Since $a \equiv b \pmod{n}$, then $n|(a - b)$. Apply the FTA to write $a - b = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, $m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, and $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$. Applying Problem 2 twice, we conclude that $s_i \le r_i$ and $t_i \le r_i$, for all i. But then $\max(s_i, t_i) \le r_i$, for all i. Applying problem 3, we conclude that $\operatorname{lcm}(m, n)|(a - b)$. Hence $a \equiv b \pmod{\operatorname{lcm}(a, b)}$.
$\leftarrow$: Since $a \equiv b \pmod{\operatorname{lcm}(m, n)}$, then $\operatorname{lcm}(m, n)|(a - b)$. But since $\operatorname{lcm}(m, n)$ is a multiple of m, in fact $m|(a - b)$. Similarly $\operatorname{lcm}(m, n)$ is a multiple of n, so in fact $n|(a - b)$. Hence $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.