MATH 521A: Abstract Algebra
Exam 1 Solutions

1. Let $p \in \mathbb{N}$ be irreducible, with $p > 4$. Use the Division Algorithm to prove that p is of the form $6k+1$ or $6k+5$ for some integer k.

   Apply the division algorithm to $p, 6$ to get integers k, r with $p = 6k + r$ and $0 \le r < 6$. If $r = 0$, then $6|p$, which is impossible as p is irreducible. If $r = 2$, then $p = 2(3k+1)$, so $2|p$, which is impossible as p is irreducible with $p > 4$. If $r = 3$, then $p = 3(2k+1)$, so $3|p$, which is again impossible. Lastly, if $r = 4$, then $p = 2(3k+2)$, so again $2|p$, which is again impossible.

2. Use the extended Euclidean Algorithm to find $\gcd(119, 175)$ and to find $x, y \in \mathbb{Z}$ with $119x + 175y = \gcd(119, 175)$.

   Step 1: $175 = 1 \cdot 119 + 56$. Step 2: $119 = 2 \cdot 56 + 7$. Now $56 = 7 \cdot 8$, so we conclude that $\gcd(119, 175) = 7$. Step 3: $7 = 119 - 2 \cdot 56$. Step 4: $7 = 119 - 2 \cdot (175 - 1 \cdot 119) = 3 \cdot 119 - 2 \cdot 175$. Hence we have $x = 3, y = -2$.

3. Apply the Miller-Rabin test to $n = 63$ and $a = 2$, and interpret the result.

   We have $n-1 = 62 = 2^1 \cdot 31$, so $s = 1$ and $d = 31$. Hence we calculate $2^{31} \pmod{63}$. We can do this by hand: $2^{31} = (2^6)^5 2^1$, and $2^6 = 64 \equiv 1 \pmod{63}$. Hence $2^{31} \equiv 1^5 \cdot 2 = 2 \pmod{63}$. Since this is neither 1 nor 62, we conclude that $a = 2$ is a witness to n being composite.

4. Let $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$. Without using the FTA, prove that $\gcd(a, b^2) = 1$.

   Direct Solution: Set $d = \gcd(a, b^2)$, and set $f = \gcd(d, b)$. We have $f|b$ and $f|a$ (since $f|d$ and $d|a$), so $f|\gcd(a, b)$. But $\gcd(a, b) = 1$, so $f = 1$. Now, we apply Theorem 1.4 [which states that if $d|x \cdot y$ and $\gcd(d, x) = 1$, then $d|y$] with $x = y = b$. Since $f = 1$, we conclude that $d|b$. But also $d|a$, so $d|\gcd(a, b)$, so $d = 1$.

   Alternate Solution: Apply Theorem 1.2 to get integers u, v with $au+bv = \gcd(a, b) = 1$. We square both sides to get $1 = a^2u^2 + 2aubv + b^2v^2 = a(a^2u^2 + 2ubv) + b^2(v^2)$. Since $a^2u^2 + 2ubv, v^2 \in \mathbb{Z}$, we have $1 \in$PLC(a, b^2). Since no positive integer is less than 1, in fact 1 is the minimal element of PLC(a, b^2), which is $\gcd(a, b^2)$ by Thm 1.2 again.

5. Prove that $S = \mathbb{N} \cup \{\pi\}$ is well-ordered.

   The usual order is NOT recommended, as that leads to many cases. Recommended is an order which puts π at one end, like $\pi \prec 1 \prec 2 \prec 3 \prec \cdots$. Now, let $T \subseteq S$. If T contains π, then π is the minimal element of T by the way we built the order $\prec$. If T does not contain π, then $T \subseteq \mathbb{N}$, and $\prec$ agrees with the usual order $<$ on $\mathbb{N}$, so T has a minimal element since $\mathbb{N}$ is well-ordered by $<$.

6. Prove the following variant of the division algorithm: Let a, b be integers with $b > 0$. then there exist (not necessarily unique) integers q, r such that $a = bq + r$ and $-1 \leq r \leq b - 2$.

   Set $S = \{a - bx : x \in \mathbb{Z}, a - bx \geq -1\}$. Step 1: We prove $S \neq \emptyset$. Take $x = -|a|$, and calculate $a - bx = a + b|a| \geq 0$. Hence $a - bx \in S$. Step 2: $S \subseteq \{-1\} \cup \mathbb{N}_0$, which we proved was well-ordered (by the usual order) in the first homework. Hence, there is some minimal element r in S. Since $r \in S$, we have $r \geq -1$. Step 3: We prove that $r \leq b - 2$. We argue by contradiction; if instead $r \geq b - 1$, then $r - b = a - b(q + 1)$ would be a smaller element of S, which is impossible.

7. Let $a, b, c, d \in \mathbb{Z}$ with $a|c$, $b|c$, and $\gcd(a, b) = d$. Without using the FTA, prove that $ab|cd$.

   Direct Solution: For some integers a', b', we have $a = da', b = db'$, since $d = \gcd(a, b)$. In fact $\gcd(a', b') = 1$ (else d would be larger). Since $a|c$, there is some integer f with $c = af = da'f$. Since $b|c$, there is some integer g with $db'g = bg = da'f$. Cancelling, we get $b'g = a'f$. So $b'|a'f$, but $\gcd(b', a') = 1$, so by Theorem 1.4 we must have $b'|f$. Hence there is some integer k with $f = b'k$. We now have $cd = (af)d = a(b'kd) = (ab)k$, so $ab|cd$.

   Alternate Solution: Apply Theorem 1.2 to get integers u, v with $au+bv = \gcd(a, b) = d$. Now, since $a|c$, there is some integer e with $c = ae$. Since $b|c$, there is some integer f with $c = bf$. We now multiply $au+bv = d$ on both sides by c to get $cau+cbv = cd$, then substitute twice to get $(bf)au + (ae)bv = cd$. Rearranging, we get $ab(fu + ev) = cd$. Since $fu + ev \in \mathbb{Z}$, in fact $ab|cd$.

8. Let $a, b, c \in \mathbb{Z}$ with $ab = c^2$ and $\gcd(a, b) = 1$. Prove that a, b are perfect squares.

   Apply the FTA. Let $p_1, \ldots, p_k$ be all the positive primes dividing any of a, b, c. We have $a_i, b_i, c_i \in \mathbb{N}_0$ with $a = \prod p_i^{a_i}, b = \prod p_i^{b_i}, c = \prod p_i^{c_i}$, where all the products are from $i = 1$ to k. The relationship $ab = c^2$ gives us k equations: $a_i + b_i = 2c_i$, for $1 \leq i \leq k$. Since $\gcd(a, b) = 1$, then for each $i \in [1, k]$, we must have either $a_i = 0$ or $b_i = 0$ (else p_i would be a common divisor of a, b). Hence, for each $i \in [1, k]$, either $a_i = 2c_i$ or $b_i = 2c_i$. Hence all of the exponents a_i and b_i are even, which means that a, b are both perfect squares.