HOMEWORK 2 SOLUTIONS

MATT RATHBUN
MATH 310, SECTION 3
ABSTRACT ALGEBRA

1.3 #2, 6, 13, 23; 2.1 #2, 8, 11, 27

Section 1.3.

2. Suppose that \( p \) is prime, and let \( a \) be an integer. Then \((a, p)\) is a positive divisor of \( p \), so it is either 1 or \(|p|\). If it is 1, then we are done. Otherwise, \(|p|\) is a divisor of \( a \), so \( p|a \) as well.

Conversely, suppose that for any \( a \in \mathbb{Z} \), either \((a, p) = 1\) or \( p|a \). Let us suppose, by way of contradiction, that \( p \) is not prime. Then \( p \) has a non-trivial factorization into primes, \( p = p_1 \cdot p_2 \cdots p_k \) for some \( k \geq 2 \). Let \( 1 \leq l < k \). Suppose \( a = p_1 \cdot p_2 \cdots p_l \). Since \( l < k \), \( p \not| a \). But \((a, p) = ((p_1 \cdots p_l), (p_1 \cdots p_k)) = p_1 \cdots p_l \neq 1\). This contradicts our hypothesis, so \( p \) must be prime.

6. Suppose \( p \) is prime and \( p|a^n \). Then by Corollary 1.9, \( p|a \), so \( p^n|a^n \).

13. Consider the factorizations of \( a \) and \( b \) into primes: \( a = p_1^{n_1} \cdots p_r^{n_r}, \ b = q_1^{m_1} \cdots q_s^{m_s}, \) with \( n_i, m_j \geq 1 \). Then \( c^2 = ab = p_1^{n_1} \cdots p_r^{n_r} \cdot q_1^{m_1} \cdots q_s^{m_s} \). Taking the square root of both sides, we arrive at \( c = p_1^{m_1} \cdots p_r^{m_r} \cdot q_1^{m_1} \cdots q_s^{m_s} \). Since \( c \) is still an integer, the product on the right must be an integer as well. Since \( (a, b) = 1 \), none of the \( p_i \) are the same as any of the \( q_j \), so it must be the case that each exponent \( n_i \) and \( m_j \) is even. But this says exactly that \( a = p_1^{m_1} \cdots p_r^{m_r} = (p_1^{m_1/2} \cdots p_r^{m_r/2})^2 \) and \( b = q_1^{m_1} \cdots q_s^{m_s} = (q_1^{m_1/2} \cdots q_s^{m_s/2})^2 \) are perfect squares.

23. Suppose there were a finite number of primes, \( p_1, \ldots, p_k \). Then consider the number \( n = (p_1 p_2 \cdots p_k) + 1 \). For each prime \( p_i \), \( n = p_i (p_i \cdots p_{i-1} \cdots p_1 \cdots p_k) + 1 \), so the Division Algorithm tells us that \( p_i \not| n \). But \( p_1, \ldots, p_k \) is supposed to be an exhaustive list of all the primes, and none of them divides \( n \). This contradicts the Fundamental Theorem of Arithmetic, so there must be infinitely many primes.

Section 2.1.

2.

(a) \( k \equiv 1 \pmod{4} \Rightarrow k - 1 = 4r \) for some \( r \in \mathbb{Z} \Rightarrow k = 4r + 1 \).

So \( 6k + 5 = 6(4r + 1) + 5 = 24r + 11 \equiv 11 \equiv 3 \pmod{4} \).

(b) \( r \equiv 3 \pmod{10} \Rightarrow r - 3 = 10a \) for some \( a \in \mathbb{Z} \), and \( s \equiv -7 \pmod{10} \Rightarrow s + 7 = 10b \) for some \( b \in \mathbb{Z} \).

Then, \( r = 3 + 10a, s = -7 + 10b \).

So, \( 2r + 3s = 2(3 + 10a) + 3(-7 + 10b) = 20a + 30b - 27 \equiv -27 \equiv -15 \equiv 5 \pmod{10} \).

8.

(a) \( 2^{5-1} = 2^4 = 16 \equiv 1 \pmod{5} \).

(b) \( 4^{7-1} = 4^6 = 4096 \equiv 1 \pmod{7} \).

(c) \( 3^{11-1} = 3^{10} = 59049 \equiv 1 \pmod{11} \).

11.

(a) \{4\}

(b) \{5\}

(c) \{4,9,14\}

(d) \emptyset
27.
(a) The statement is false. $2 \cdot 3 \equiv 0 \pmod{6}$, but $2 \not\equiv 0 \pmod{6}$, nor $3 \not\equiv 0 \pmod{6}$.
(b) The statement is true when $n$ is prime. Suppose $n$ is prime and $ab \equiv 0 \pmod{n}$. Then $n|ab$. By Theorem 1.8, $n|a$ or $n|b$, which means either $a \equiv 0 \pmod{n}$, or $b \equiv 0 \pmod{n}$. 