Homework Set #2

§1.2 #8 Let a, b be positive integers and $d = (a,b)$. Then $a = hd$ and $b = kd$ for integers h and k. Show $(h,k) = 1$.

Proof: We can write $d = ma + nb = mhd + nkd = (mh + nk)d$, and hence $1 = mh + nk$. This is clearly the smallest positive linear combination of h and k, so $(h,k) = 1$. //

§1.2 #16 An integer $a > 1$ is a square iff every exponent in its prime factorization is even.

Proof: Suppose $a = n^2$. Then $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ for primes $p_1 < \cdots < p_k$ and exponents $\alpha_i > 0$. Hence $a = p_1^{2\alpha_1} \cdots p_k^{2\alpha_k}$ is the prime factorization of a (by uniqueness) and has all exponents even.

Conversely, if $a = p_1^{2\alpha_1} \cdots p_k^{2\alpha_k}$ then $a = (p_1^{\alpha_1} \cdots p_k^{\alpha_k})^2$. //

§1.3 #6 Find all integers x for which $3x + 7$ is divisible by 11.

Solution: $11 \mid 3x+7 \iff 3x + 7 \equiv 0 \ (11) \iff 3x \equiv -7 \equiv 4 \ (11) \iff 4(3x) \equiv 16 \ (11) \iff x \equiv 5 \ (11)$. Hence the solutions are the integers $5 + 11q$, $q \in \mathbb{Z}$. //

§1.3 #7 Find additive orders of some elements, as follows.

(a) 8 mod 12: $8x \equiv 0 \ (12) \iff x \equiv 0 \ (3)$ so $\underline{x = 3}$

(b) 7 mod 12: $7x \equiv 0 \ (12) \iff x \equiv 0 \ (12)$ so $\underline{x = 12}$

(c) 21 mod 28: $21x \equiv 0 \ (28) \iff 3x \equiv 0 \ (4) \iff x \equiv 0 \ (4)$ so $\underline{x = 4}$

(d) 12 mod 18: $12x \equiv 0 \ (18) \iff 2x \equiv 0 \ (3) \iff x \equiv 0 \ (3)$ so $\underline{x = 3}$

§1.3 #8 If p is prime and $p \nmid a$, then the additive order of a mod p is p.

Proof: It is necessary to find the least positive x such that $ax \equiv 0 \ (p)$. But this means $p \mid ax$, and since $p \nmid a$ it follows that $p \mid x$. Hence the smallest positive x is p. That is, the order of a is p. //