Chapter 0 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

February 20, 2014

Problem 7

Show that if a and b are positive integers, then $ab = \text{lcm}(a, b) \cdot \gcd(a, b)$.

An argument is made here based upon the prime factorizations of $ab/\gcd(a, b)$ and $\text{lcm}(a, b)$. The latter may be thought of as the union of two sets A and B. The former, in terms of these sets, may be thought of as the left-hand side of the following equation.

$$(A - B) \cup (B - A) \cup (A \cap B) = A \cup B$$

The set A contains primes in the prime factorization of a, and B contains primes in the prime factorization of b. The proof goes through by the equality of the equation above.

This proof is not precise, but the intuition is correct, I believe.

Problem 9

If a and b are integers and n is a positive integer, prove that $a \equiv b \pmod{n}$ if and only if n divides $a - b$.

Let $a = nq_a + r_a$ and $b = nq_b + r_b$. If $r_a = r_b$, then $a - b = n(q_a - q_b)$, showing that $n|(a - b)$.

Now let $a = nq_a + r_a$ and $b = nq_b + r_b$ again and write

$$a - b = n(q_a - q_b) + r_a - r_b.$$

Now since $n|(a-b)$, we must have $n|(r_a - r_b)$ so that there exists an integer k such that $r_a = r_b + nk$. But since $0 \leq r_a, r_b < n$, we have $|r_a - r_b| < n$, and therefore, $k = 0$. It follows that $r_a = r_b$.

Problem 10

Let $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.

Let $u, v \in \mathbb{Z}$ be integers such that $d = au + bv$. Then $1 = (a/d)u + (b/d)v$. Then, by Theorem 0.2, we have $\gcd(a', b') = 1$, because there is no smaller positive integer than 1.

Problem 11

Let n be a fized positive integer greater than 1. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, prove that $a + b \equiv a' + b' \pmod{n}$ and $ab = a'b' \pmod{n}$.

Letting $a' = a + k_a n$ and $b' = b + k_b n$, we find that

$$a' + b' = a + b + n(k_a + k_b),$$

and that

$$a'b' = ab = n(ak_b + bk_a + k_a k_b n),$$

showing that n divides both $a'b' - ab$ and $a' + b' - (a + b)$. The proof now goes through by Problem 9.

Problem 12

Let a and b be positive integers and let $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. If t divides both a and b, prove that t divides d. If s is a multiple of both a and b, prove that s is a multiple of m.

By Theorem 0.2, d is a linear combination of a and b, and therefore, any common divisor of a and b, such as t, also divides d.

To see that m divides s, simply notice that all common multiples of a and b are generated by all positive multiples of m.

Problem 13

Let n and a be positive integers and let $d = \gcd(a, n)$. Show that the equation $ax \equiv 1 \pmod{n}$ has a solution if and only if $d = 1$.

If $d = 1$, there exist integers $u, v \in \mathbb{Z}$ such that $1 = au + nv$, showing that n divides $1 - au$. Letting $x = u$, the equation in x above has a solution by Problem 9.

Now suppose the equation above has a solution in x. Then n divides $1 - ax$ and there exists $v \in \mathbb{Z}$ such that $1 = nv + ax$. It now follows that $d = 1$ by Theorem 0.2, because there is no positive integer smaller than 1.

Problem 15

Let a, b, s and t be integers. If $a \equiv b \pmod{st}$, show that $a \equiv b \pmod{s}$ and $a \equiv b \pmod{t}$. What condition on s and t is needed to make the converse true?

By symmetry of the problem, we need only show that $a \equiv b \pmod{s}$. Notice that $s|st$ and $st|(b - a)$ by Problem 9. It follows that $s|(b - a)$, and we're done by Problem 9.

Suppose now that $a \equiv b \pmod{t}$ and $a \equiv b \pmod{s}$. Then $s|(b - a)$ and $t|(b - a)$, from which it is clear that if $\gcd(a, b) = 1$, then $st|(b - a)$, but this is a sufficient condition, not a necessary one.

Problem 17

Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

If a shares no prime factors in common with b and c, then it clearly doesn't share any prime factors in common with bc. Conversley, if a shares no prime factors in common with bc, then it certainly doesn't share any prmie factors in common with b and c.

Problem 24

(Generalized Euclid's Lemma) If p is a prime and p divides $a_1 a_2 \dots a_n$, prove that p divides a_i from some i.

The case $n = 2$ is covered by Euclid's Lemma. Now suppose, for a fixed integer $k > 2$, that the generalized lemma holds in the case $n = k - 1$. Now consider the case $n = k$. If p does not divide a_n, then clearly p divides $a_1 a_2 \ldots a_{n-1}$ by Euclid's Lemma. Then, by our inductive hypothesis, p must divide a_i for an integer $i \in [1, n-1]$. We have now proven the general lemma by the principle of mathematical induction.

Problem 25

Use the Generalized Euclid's Lemma (see Exercise 24) to establish the uniqueness portion of the Fundamental Theorem of Arithmetic.

Suppose an integer n has two different prime factorizations $p_1^{a_1} \ldots p_r^{a_r}$ and $q_1^{b_1} \ldots q_s^{b_s}$. By the Generalized Euclid's Lemma, if $p \in \{p_i\}_{i=1}^r$, then $p \in \{q_i\}_{i=1}^s$, because p divides n. Conversely, if $p \in \{q_i\}_{i=1}^s$, then $p \in \{p_i\}_{i=1}^r$ by the same reason. It follows that $\{p_i\}_{i=1}^r = \{q_i\}_{i=1}^s$, which is a contradiction, and therefore, no integer n has two different prime factorizations.