Homework 3
Section 1.3

Jonathan Petersen
A01236750

January 27th, 2016

---

7. **If $a, b, c \in \mathbb{Z}$ and p is a prime such that $p|a$ and $p|a + bc$, prove that $p|b$ or $p|c$.**

   Because $p|a$ we know that

   $$a = pk \qquad k \in \mathbb{Z} \tag{1}$$

   By the same logic, we can see that

   $$a + bc = pl \qquad l \in \mathbb{Z} \tag{2}$$

   If we substitute for a in equation 2, we find that

   $$\begin{aligned} pk + bc &= pl \\ bc &= pl - pk \\ bc &= p(l - k) \\ bc &= pm \qquad m = l - k \therefore m \in \mathbb{Z} \end{aligned}$$

   Therefore $p|bc$. Finally, by Theorem 1.5, it must be that $p|b$ or $p|c$ ■

15. **If p is prime and $p|a^n$, is it true that $p^n|a^n$? Justify your answer.**

    Given a prime number p such that $p|a^n$ for some $n \in \mathbb{Z}$, then by Collorary 1.6 it must be that $p|a$. It then follows that:

    $$\begin{aligned} a &= kp \qquad k \in \mathbb{Z} \\ a^n &= (kp)^n \\ a^n &= lp^n \qquad l = k^n \therefore l \in \mathbb{Z} \end{aligned}$$

    Which, by definition, means that $p^n|a^n$ ■

21. **If $c^2 = ab$ and $gcd(a, b) = 1$, prove that a, b are perfect squares.**

By the funamental theorem of arithmatic, it must be that

$$\begin{aligned}
a &= q_1^{u_1} * q_2^{u_2} * ... * q_n^{u_n} \qquad q \text{ is prime} \qquad u \in \mathbb{Z} \\
b &= r_1^{v_1} * r_2^{v_2} * ... * r_n^{v_n} \qquad r \text{ is prime} \qquad v \in \mathbb{Z} \\
c &= p_1^{t_1} * p_2^{t_2} * ... * p_n^{t_n} \qquad p \text{ is prime} \qquad t \in \mathbb{Z} \\
c^2 &= p_1^{2t_1} * p_2^{2t_2} * ... * p_n^{2t_n} \\
ab = c^2 &= p_1^{2t_1} * p_2^{2t_2} * ... * p_n^{2t_n}
\end{aligned}$$

Furthermore, since $gcd(a, b) = 1$, we know that a and b have no factors in common greater than 1, including prime factors. Therefore, the prime factors of a and b individually must form a basis or partition of the factors of ab, with no overlapping factors. Or, put another way, that a and b can both be expressed using some subset of the prime factors of ab, with both subsets being disjoint.

Observe now that every factor in the prime factorization of ab is a perfect square number. By the properties of multiplication, any product of square numbers must also be a square number, therefore no matter the factors of ab are partioned into the factors of a and b, a and b must be square numbers themselves $\blacksquare$

25. **Let p be prime and $1 \le k < p$. Prove that p divides the binomial coefficient $\binom{p}{k}$.**

Given p, k as described in the statement, observe that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

Because $1 \le k < p$, we know that none of the terms in the denominator will ever cancel with the factor of p in the numerator. $k!$ cannot cancel with it because $k < p$, and $(p - k)!$ cannot cancel with it because $k > 0$, so $(p - k) < p$. Therefore we can rewrite the equation as

$$\begin{aligned}
\binom{p}{k} &= \frac{p(p-1)!}{k!(p-k)!} \\
&= p\frac{(p-1)!}{k!(p-k)!} \\
&= pn \qquad n = \tfrac{(p-1)!}{k!(p-k)!} \therefore n \in \mathbb{Z}
\end{aligned}$$

Which, by definition, means that $p|\binom{p}{k}$ $\blacksquare$

26. **If n is a positive integer, prove that there exist n consecutive composite integers.**

Let

$$S = \{(n+1)!+0, (n+1)!+1, (n+1)+2, ..., (n+1)!+k\} \qquad n, k \in \mathbb{Z} \qquad k = n-1$$

It is obvious that the elements of S must be consecutive integers, and that S must contain $k+1 = n$ entries, so all that remains is to prove that every element in S is composite.

Let us consider an arbitrary element of S,

$$\begin{aligned} s &= (n+1)! + i \qquad 0 \leq i < n \qquad i \in \mathbb{Z} \\ &= (n * n-1 * n-2 * ... * i * ... * 2 * 1) + i \\ &= ij + i \qquad ij = (n+1)! \therefore j \in \mathbb{Z} \\ &= i(j+1) \end{aligned}$$

And since addition is closed over the integers, $j+1 \in \mathbb{Z}$, so $i|s$ for all s. This means that s is composite, and by extension S is a collection of n consecutive composite numbers ■

31. **If p is a positive prime, prove that $\sqrt{p}$ is irrational.**

We will prove by contradiction. That is, hypothesize that there exists p such that:

$$\begin{aligned} \sqrt{p} &= \frac{a}{b} \qquad a, b \in \mathbb{Z} \qquad gcd(a, b) = 1 \\ p &= (\frac{a}{b})^2 \end{aligned}$$

We immediately see that

$$\begin{aligned} p = (\frac{a}{b})^2 \implies b^2 p &= a^2 \\ kp &= a^2 \qquad k = b^2 \therefore k \in \mathbb{Z} \end{aligned}$$

Which by definition means that $p|a^2$, and by Theorem 1.5 means that $p|a$. Using this fact, it follows that

$$
\begin{aligned}
b^2p &= a^2 \\
b^2p &= (pk)^2 \\
b^2p &= p^2k^2 \\
b^2 &= pk^2 \\
b^2 &= pl \qquad l = k^2 \therefore k \in \mathbb{Z}
\end{aligned}
$$

Which again means that $p|b^2$ and therefore $p|b$. However, this is a contradiciton! If $p|a$ and $p|b$, then $gcd(a, b) \neq 1$, contrary to the given hypothesis. Therefore, the hypothesis must be false, and it must needs be that if p is a positive prime then $\sqrt{p}$ is irrational. ∎