Solution for Math 301 Homework 2

Section 1.2

1. Find the greatest common divisor using Euclid's algorithm.

d) $(143, 231)$

	143	231	1
1	88	143	
1	55	88	1
	33	55	
2	22	33	1
	22	22	
	0	11	1

$\Rightarrow \qquad (143, 231) = 11.$

h) $(12378, 3054)$

4	12378	3054	18
	12216	2916	
1	162	138	5
	138	120	
1	24	18	3
	18	18	
	6	0	

$\Rightarrow \qquad (12378, 3054) = 6$

4.

a) If $a|b$ and $a|c$, prove that $a|(b+c)$.

Suppose $a|b$ and $a|c$. Then $b = ax$, $c = ay$ for some $x, y \in \mathbb{Z}$. We have

$$(b+c) = ax + ay = a(x+y) \Rightarrow a|(b+c).$$

b) If $a|b$ and $a|c$, prove that $a|(br+ct)$ for any $r, t \in \mathbb{Z}$.

Suppose $a|b$ and $a|c$. Then $b = ax$, $c = ay$ for some $x, y \in \mathbb{Z}$. Let $r, t \in \mathbb{Z}$. We have

$$(br+ct) = axr + ayt = a(xr+yt) \Rightarrow a|(br+ct).$$

22. If $(a, c) = 1$ and $(b, c) = 1$, prove that $(ab, c) = 1$.

Suppose $(a, c) = 1$ and $(b, c) = 1$. Then there exist $u, v, x, y \in \mathbb{Z}$ such that

$$\begin{aligned} & au + cv = 1, \ bx + cy = 1 \\ \Rightarrow \ & (au+cv)(bx+cy) = 1 \\ \Rightarrow \ & ab(ux) + c(auy + vbx + vcy) = 1 \\ \Rightarrow \ & (ab, c) = 1 \end{aligned}$$

24. Let $a, b, c \in \mathbb{Z}$. Prove that the equation $ax + by = c$ has integer solutions if and only if $(a, b)|c$.

Let $a, b, c \in \mathbb{Z}$. Suppose $d = (a, b)$. Then $a = dr$ and $b = ds$ for some $r,\ s \in \mathbb{Z}$.

If $ax + by = c$ for some $x, y \in \mathbb{Z}$, then $drx + dsy = c \Rightarrow c = d(rx + sy) \Rightarrow d|c$

Suppose $d|c$. Then $c = dt$ for some $t \in \mathbb{Z}$. Let $u, v \in \mathbb{Z}$ such that

$$au + bv = d \Rightarrow a(ut) + b(vt) = dt = c.$$

Section 1.3

14. Let p be an integer other than $0, \pm 1$ with this property: Whenever b and c are integers such that $p|bc$, then $p|b$ or $p|c$. Prove that p is prime.
Hint: If d is a divisor of p, say $p = dt$, then $p|d$ or $p|t$. Show that this implies $d = \pm p$ or $d = \pm 1$.

Let p be an integer other than $0, \pm 1$ with the given property. Suppose $d|p$. Then $p = dt$ for some $t \in \mathbb{Z}$. Hence, $p|dt \Rightarrow p|d$ or $p|t$. Consider the following cases:

1) $p|d \Rightarrow d = pr$ for some $r \in \mathbb{Z}$. We have

$$p = dt = (pr)t = p(rt) \Rightarrow rt = 1 \Rightarrow r = t = 1 \text{ or } r = t = -1.$$

We have $d = \pm p$.

2) $p|t \Rightarrow t = ps$ for some $s \in \mathbb{Z}$. We have

$$p = dt = d(ps) = p(ds) \Rightarrow 1 = ds \Rightarrow d = s = 1 \text{ or } d = s = -1.$$

We have $d = \pm 1$
Since, $d|p \Rightarrow d = \pm p$ or $d = \pm 1$, p is a prime.

22. Let $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where p_i are distinct primes and each $r_i > 0$. Prove that n is a perfect square if and only if each r_i is even.

Let $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, where $p_1,\ p_2,\ \ldots p_k$ are distinct primes and each $r_i > 0$.
If each r_i is even, then $r_i = 2s_i$ for some $s_1,\ s_2,\ \ldots s_k \in \mathbb{Z}$. We have

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} = p_1^{2s_1} p_2^{2s_2} \cdots p_k^{2s_k} = \left(p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}\right)^2 \text{ is a perfect square.}$$

Conversely, suppose $n = a^2$ for some $a \in \mathbb{Z}$. Since $p_1,\ p_2,\ \ldots p_k$ are distinct primes and each $r_i > 0$, we have $1 < n = a^2 = |a|^2$. Therefore, $|a| > 1$ and we can write $a = q_1^{s_1} q_2^{s_2} \cdots q_h^{s_h}$ where $q_1,\ q_2,\ \ldots q_h$ are distinct primes and each $s_i > 0$. Then

$$p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} = n = a^2 = q_1^{2s_1} q_2^{s_2} \cdots q_h^{2s_h}.$$

By the uniqueness in prime factorization of n, we have $k = h$ and by a rearrangement of indices, we can assume that $p_i = q_i$ and $r_i = 2s_i$ for all $1 \leqslant i \leqslant k$. Hence, all r_i are even.

30.

a) Prove that there are no nonzero integers a, b such that $a^2 = 2b^2$.
Hint: Use the Fundamental Theorem of Arithmetic.

We will prove by contradiction. Suppose a, b are nonzero integers such that $a^2 = 2b^2$. By the result in Ex. 22, we have distinct primes $p_1, p_2, \ldots p_k$ and integers $s_1, s_2, \ldots s_k > 0$ such that $a^2 = p_1^{2s_1} p_2^{2s_2} \cdots p_k^{2s_k}$ and distinct primes $q_1, q_2, \ldots q_h$ and integers $t_1, t_2, \ldots t_h > 0$ such that $b^2 = q_1^{2t_1} q_2^{2t_2} \cdots q_h^{2t_h}$. Since $a^2 = 2b^2$, we have $2 | a^2 \Rightarrow p_i = 2$ for some i. Then we have

$$p_1^{2s_1} p_2^{2s_2} \cdots p_k^{2s_k} = 2 q_1^{2t_1} q_2^{2t_2} \cdots q_h^{2t_h}$$

Therefore, the power of the prime 2 on the left hand side is even but odd on the right hand side, a contradiction.

b) Prove that $\sqrt{2}$ is irrational.
Hint: Use proof by contradiction (Appendix A). Assume that $\sqrt{2} = a/b$ (with $a, b \in \mathbb{Z}$) and use part (a) to reach a contradiction.

If $\sqrt{2}$ is rational, then there exist nonzero integers $a, b \in \mathbb{Z}$ such that

$$\frac{a}{b} = \sqrt{2} \Rightarrow a^2 = 2b^2,$$

a contradiction to the result in (a).

34. Prove or disprove: If n is an integer and $n > 2$, then there exists a prime p such that $n < p < n!$.

We are going to prove that if n is an integer and $n > 2$, then there exists a prime p such that $n < p < n!$.

$$n > 2 \Rightarrow n! \geqslant n(n-1) \geqslant 2n > n + 1 \Rightarrow n! > n! - 1 > n > 2.$$

vskip.1in
Choose a positive prime p such that $p | (n! - 1)$. Then $n! - 1 = pk$ for some positive integer k. We have $\boxed{p \leqslant n! - 1 < n!}$. Since $n! = kp + 1$, we have

$$p \nmid n! \Rightarrow (n!, p) = 1 \Rightarrow p \neq m \text{ for all } 1 \leqslant m \leqslant n$$

vskip.1in (because $m | n!$ for all $1 \leqslant m \leqslant n$). Therefore, $\boxed{n < p}$. Hence, $n < p < n!$.

36. Let $p = 12m + r$, where $m, r \in \mathbb{Z}$ and $0 \leqslant r < 12$. We have

$$\begin{cases} 2|p & \text{if } r = 0,\ 2,\ 4,\ 6,\ 8,\ 10 \\ 3|p & \text{if } r = 0,\ 3,\ 6,\ 9. \end{cases}$$

Since $p \geqslant 5$ is a prime, we have $r = 1, 5, 7, 11 \Rightarrow r^2 = 1, 25, 49, 121$. Hence, $r^2 = 24k + 1$, where $k = 0, 1, 2, 5$ respectively. So we have

$$p^2 = (12m + r)^2 = 144m^2 + 24mr + r^2 = 24(6m^2 + mr + k) + 1 = 24x + 1,$$

for some $x \in \mathbb{Z}$. Similarly, $q^2 = 24y + 1$ for some $y \in \mathbb{Z}$. Hence, $p^2 - q^2 = 24(x - y)$ is divisible by 24.