Math 300.2 **Problem Set 8 Answers** **Fall, 2007**

1. (a) [Proposition 2.2.32.] Write

$$m = q\,n + r$$

with $0 \le r < n$, so that $r = m \bmod n$. Let d be a positive integer. If d is a common divisor of m and n, then $d \mid r = m - q\,n$; conversely, if d is a common divisor of n and r, then $d \mid q\,n + r = m$. Thus the common divisors of m and n are exactly the same as the common divisors of n and r. $\square$

(b) [Exercise 2.2.36 (a).]

$$\begin{aligned} 156 &= 3 \cdot 42 + 30 & \Longrightarrow \quad 30 &= 156 - 3 \cdot 42 \\ 42 &= 1 \cdot 30 + 12 & \Longrightarrow \quad 12 &= 42 - 1 \cdot 30 \\ 30 &= 2 \cdot 12 + 6 & \Longrightarrow \quad 6 &= 30 - 2 \cdot 12 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

Hence

$$\boxed{\gcd(156, 42) = 6}$$

and

$$\begin{aligned} 6 &= 30 - 2 \cdot (42 - 1 \cdot 30) = 3 \cdot 30 - 2 \cdot 42 \\ &= 3 \cdot (156 - 3 \cdot 42) - 2 \cdot 42 = 3 \cdot 156 - 11 \cdot 42 \\ &= 3 \cdot 156 + (-11) \cdot 42 \end{aligned}$$

so that

$$\boxed{6 = 3 \cdot 156 + (-11) \cdot 42}$$

2. [Corollary 2.2.39.] Assume $a \mid n$ and $b \mid n$; this means there are integers k and d with

$$n = k\,a, \qquad n = d\,b.$$

Since by hypothesis the integers a and b are relatively prime, there are integers s and t with

$$1 = a\,s + b\,t.$$

Multiply by n to obtain

$$n = n\,a\,s + n\,b\,t.$$

In this equation, substitute $d\,b$ for n in the first term on the right-hand side and $k\,a$ for n in the second term to obtain:

$$\begin{aligned} n &= (d\,b)\,a\,s + (k\,a)\,b\,t \\ &= (a\,b)\,(d\,s) + (a\,b)\,(k\,t) \\ &= (a\,b) \cdot (d\,s + k\,t). \end{aligned}$$

Since $a\,b$ divides the right-hand side above, it divides the left-hand side, n. $\square$.

3. [**Extra credit:** [Exercise 2.2.40 (2).] Let d be a common divisor of $m+n$ and $m-n$. Then d divides $(m+n)+(m-n) = 2\,m$ and d divides $(m+n)-(m-n) = 2\,n$.

   Suppose first that d is even, so that $d = 2\,k$ for some integer k. Then $2\,k \mid 2\,m$ so that $k \mid m$, and similarly, $k \mid n$. Then $k = 1$ because m and n are relatively prime. Hence $d = 2$.

   Suppose now that d is odd. Then 2 and d are relatively prime. Since $d \mid 2\,m$, then (by Proposition 2.2.38) $d \mid m$. Similarly, $d \mid n$. Since m and n are relatively prime, $d = 1$. $\square$

4. [Lemma 2.3.8.] Let p be a prime. We use induction on n to prove that, for every n-tuple $(q_1, q_2, \ldots, q_n)$ of primes, if $p \mid \prod_{j=1}^{n} q_j$, then $p = q_j$ for some j with $1 \leq j \leq n$.

   Base step ($n = 1$): If q_1 is a single prime, so that $\prod_{j=1}^{1} q_j = q_1$, and if $p \mid q_1$, then $p = q_1$ by definition of "prime".

   Inductive step: Now let $n \geq 1$ and assume the statement about any n primes. Let $(q_1, q_2, \ldots, q_n, q_{n+1})$ be an $(n+1)$-tuple of primes and suppose $p \mid \prod_{j=1}^{n+1} q_j$. By the Prime Divisor Property (Proposition 2.3.7), $p \mid \prod_{j=1}^{n} q_j$ or $p \mid q_{n+1}$. In the former case, $p = q_j$ for some j with $1 \leq j \leq n$ by the inductive assumption; in the latter case, $p = q_{n+1}$ because q_{n+1} is prime. $\square$

5. [Find form (PF1) prime power representations: 1377, 50600, 1891, 547.]

   - 1377: This number is not even, so start with a trial divisor of 3 and keep dividing by 3 until you find that $3^4 \mid 1377$ and $1377 = 3^4 \cdot 17$. Since 17 is prime, the representation is:

     $$\boxed{1377 = 3^4\,17^1}$$

   - 50600: Obviously 100 is a divisor, with quotient 506, and $100 = 2^2 \cdot 5^2$. Further, 506 is even, and $506 = 2 \cdot 253$ with 253 not even. This leave the problem of factoring 253. Some trials reveal that $11 \mid 253$ and that $253 = 11 \cdot 23$. Both 11 and 23 are primes. Thus the representation is:

     $$\boxed{50600 = 2^3\,5^2\,11^1\,23^1}$$

   - 1891: This number is not even, and it has no obvious small divisors. Try dividing by successive odd primes that are less than $\sqrt{1891}$ until you find that $1891 = 31 \cdot 61$. Both 31 and 61 are prime (as you could check in various ways, e.g., by using the sieve or by trying to divide each by odd primes less than their square-roots). So the representation is:

     $$\boxed{1891 = 31^1\,61^1}$$

   - 547: This number is not even. None of the odd prime integers—3, 5, 11, 13, 17, 19, 23—that are less than $\sqrt{547}$ divide 547. This means that 547 must be prime! Hence the representation is:

     $$\boxed{547 = 547^1}$$

6. [Exercise 2.3.14 (3).] Let p be prime and just suppose $\sqrt{p}$ is rational. For some positive integers m and n,

$$\sqrt{p} = \frac{m}{n}.$$

By dividing both m and n if necessary by their greatest common divisor, we may assume without loss of generality that m and n are relatively prime.

Now

$$p\,n^2 = m^2.$$

Because $p \mid (p\,n^2)$, then $p \mid (m^2)$. From the Prime Divisor Property (Proposition 2.3.7), then $p \mid m$. Hence

$$m = p\,k$$

for some positive integer k. Then

$$p\,n^2 = (p\,k)^2 = p^2\,k^2,$$

so that

$$n^2 = p\,k^2.$$

By the same argument as before, $p \mid n$. Thus p is a common divisor of both m and n, and this is impossible. $\square$