Solution to HW 4

1.7 9.
(c) We have $36 = (-5) \cdot (-7) + 1$, so the quotient is -7 and the remainder is 1.
(d) We have $-36 = 5 \cdot (-8) + 4$, so the quotient is -8 and the remainder is 4.

1.7 11.
(c) The common divisors of 18 and -54 are 1, -1, 2, -2, 3, -3, 6, -6, 9, -9, 18, -18. We have $\gcd(18, -54) = 18$.
(d) The common divisors of -8 and -52 are 1, -1, 2, -2, 4, and -4. We have $\gcd(-8, -52) = 4$.

1.7 13. (a) We have $\gcd(13, 15) = 1 = 7 \cdot 13 - 6 \cdot 15$.
(b) We have $\gcd(26, 32) = 2 = 5 \cdot 26 - 4 \cdot 32$.
(c) We have $\gcd(9, 30) = 3 = 1 \cdot 30 - 3 \cdot 9$.

1.7 16.
Let p be a prime number and let a be a positive integer.

(a) Assume that $\gcd(p, a) = p$. Then p is a common divisor of p and a. It follows that $p \mid a$. This proves $\gcd(p, a) = p \Rightarrow p \mid a$.

Assume that $p \mid a$. Then the set of common divisors of p and a is equal to the set of divisors of p. Since p is the largest divisor of itself, it follows that $\gcd(p, a) = p$. This proves $p \mid a \Rightarrow \gcd(p, a) = p$.

We conclude that $\gcd(p, a) = p \Leftrightarrow p \mid a$.

Note: part (a) holds without the assumption that p is prime.

(b) Assume that $\gcd(p, a) = 1$. Then p is not a common divisor of p and a. It follows that $p \nmid a$. This proves $\gcd(p, a) = 1 \Rightarrow p \nmid a$.

Assume that $p \nmid a$. Since p is a prime number, the set of divisors of p is $\{-p, -1, 1, p\}$. Since p and $-p$ are not divisors of a, it follows that the set of common divisors of p and a is $\{-1, 1\}$. Therefore $\gcd(p, a) = 1$. This proves $p \nmid a \Rightarrow \gcd(p, a) = 1$.

We conclude that $\gcd(p, a) = 1 \Leftrightarrow p \nmid a$.

1.7 17.
Let q be a natural number greater than 1.
Assume that q satisfies: $\forall a, b \in \mathbb{Z} : (q \mid ab) \Rightarrow (q \mid a \bigvee q \mid b)$.
Claim: q is a prime number.
By definition this means $q > 1$ and the positive divisors of q are 1 and q.
Let $a \in \mathbb{N}$ be any positive divisor of q. We must show that $a \in \{1, q\}$.
Since $a \mid q$, we may choose $b \in \mathbb{Z}$ such that $q = ab$.
Since $a, b \in \mathbb{Z}$ and $q \mid ab$, it follows from our assumption that $q \mid a$ or $q \mid b$.
Case 1: Assume that $q \mid b$.
Then we may choose $s \in \mathbb{Z}$ such that $b = sq$.
But then $q = ab = asq$, so we must have $as = 1$.
Since a divides 1 and $a > 0$, we obtain $a = 1$.
Case 2: Assume that $q \mid a$.
Arguing as in Case 1 we deduce that $b = 1$.
Since $q = ab$, this implies that $a = q$.
Since Case 1 or Case 2 apply, we have proved that $a \in \{1, q\}$.
This finishes the proof that q is a prime number.