11. *(1 point.)* Let $d = \prod_p p^{a_p}$ be the canonical factorization of d. If $p \mid d$, then $p \mid mn$, and so p divides m or n, but not both (for otherwise $p \mid (m, n)$). Let

$$r = \prod_{\substack{p|d \\ p|m}} p^{a_p} \quad \text{and} \quad s = \prod_{\substack{p|d \\ p|n}} p^{a_p}.$$

Then clearly $rs = d$, $r \mid m$, $s \mid n$ and $(r, s) = 1$.

In other words, let $r = (d, m) \mid m$ and let $s = (d, n) \mid n$. Then, since $(m, n) = 1$, $rs = (d, mn) = d$. It is clear that $(r, s) = 1$, for if p divides (r, s) then p divides m and n, so $p \mid (m, n)$. (Or: if $m = rr'$, $n = ss'$, then we have integers x, y such that $1 = mx + ny = r(r'x) + s(s'y)$.)

14. *(2 points.)* $(x_0, y_0) = 1$ because $a/d, b/d$ are integers and $(a/d)x_0 + (b/d)y_0 = 1$, and x_0, y_0 are not unique because $a(x_0 + bt/d) + b(y_0 - at/d) = d$ for every integer t.

18.(a) *(1 point.)* If $(a, b) = (a, c) = 1$ then $[a, b] = ab$ and $[a, c] = ac$, so if $a \neq 0, b \neq c$ then $[a, b] \neq [a, c]$. For example any three distinct primes p, q, r are pairwise coprime and $[p, q] = pq, [p, r] = pr, [q, r] = qr$ are all different.

19.(a) *(1 point.)* If d divides (a, b) then it divides a, and b, hence bc, hence $(a, bc) = 1$. Hence $(a, b) = 1$. Similarly $(a, c) = 1$. Or: we have integers x, y such that $1 = ax + bcy = ax + b(cy) = ax + c(by)$, hence $(a, b) = (a, c) = 1$.

26. We claim that $(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$. Without loss of generality, assume $(a, b) = 1$. Write $m = r_0, n = r_1$, and

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 \\
r_1 &= r_2 q_2 + r_3 \\
&\vdots \\
r_{t-2} &= r_{t-1} q_{t-1} + r_t \\
r_{t-1} &= r_t q_t + 0
\end{aligned}$$

as in the Euclidean algorithm. Then $(m, n) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_t, 0) = r_t$. Now for $0 \leq i \leq t - 2$ we have

$$\begin{aligned}
a^{r_i} - b^{r_i} &= a^{r_{i+1}q_{i+1}+r_{i+2}} - b^{r_{i+1}q_{i+1}+r_{i+2}} \\
&= a^{r_{i+2}}(a^{r_{i+1}q_{i+1}} - b^{r_{i+1}q_{i+1}}) + b^{r_{i+1}q_{i+1}}(a^{r_{i+2}} - b^{r_{i+2}}) \\
&= a^{r_{i+2}}(a^{r_{i+1}} - b^{r_{i+1}})Q_{i+1} + b^{r_{i+1}q_{i+1}}(a^{r_{i+2}} - b^{r_{i+2}}),
\end{aligned}$$

where

$$Q_{i+1} = a^{r_{i+1}(q_{i+1}-1)} + a^{r_{i+1}(q_{i+1}-2)}b^{r_{i+1}} + \cdots + b^{r_{i+1}(q_{i+1}-1)}.$$

Therefore

$$(a^{r_i} - b^{r_i}, a^{r_{i+1}} - b^{r_{i+1}}) = (a^{r_{i+1}} - b^{r_{i+1}}, b^{r_{i+1}q_{i+1}}(a^{r_{i+2}} - b^{r_{i+2}})), \quad 0 \leq i \leq t - 2.$$

Now since $(a, b) = 1$, $(a^{r_{i+1}} - b^{r_{i+1}}, b^{r_{i+1}q_{i+1}}) = 1$, so

$$(a^{r_{i+1}} - b^{r_{i+1}}, b^{r_{i+1}q_{i+1}}(a^{r_{i+2}} - b^{r_{i+2}})) = (a^{r_{i+1}} - b^{r_{i+1}}, a^{r_{i+2}} - b^{r_{i+2}}).$$

Thus

$$(a^{r_0} - b^{r_0}, a^{r_1} - b^{r_1}) = (a^{r_{t-1}} - b^{r_{t-1}}, a^{r_t} - b^{r_t}).$$

Finally,

$$a^{r_{t-1}} - b^{r_{t-1}} = a^{r_t q_t} - b^{r_t q_t} = (a^{r_t} - b^{r_t})Q_t,$$

so $(a^{r_{t-1}} - b^{r_{t-1}}, a^{r_t} - b^{r_t}) = a^{r_t} - b^{r_t}$. Our claim is proved.

27. *(1 point.)* If $n+1$ divides n^2+1 then it divides $n^2+1-(n+1)(n-1) = 2$, so $n = 1$ if it is a positive integer.

39. Note that $N_k = 10^{k-1} + \cdots + 1$ and $(10-1)N_k = 10^k - 1$. Suppose $m = nq$. Then

$$10^m - 1 = (10^n - 1)(10^{n(q-1)} + 10^{n(q-2)} + \cdots + 10^n + 1) = (10^n - 1)X, \quad X = (10^{n(q-1)} + 10^{n(q-2)} + \cdots + 10^n + 1).$$

Then $(10-1)N_m = (10-1)N_n X$, that is $N_m = N_n X$, hence N_n divides N_m.

For the converse, write $m = nq + r$, $0 \le r \le n-1$. Then

$$(10-1)N_m = 10^m - 1 = 10^r(10^{nq} - 1) + 10^r - 1 = 10^r(10^n - 1)X + 10^r - 1 = 10^r(10-1)N_n X + 10^r - 1.$$

Therefore if N_n divides N_m then N_n divides $10^r - 1 \le 10^{n-1} - 1 < N_n$. Hence $10^r - 1 = 0$, that is $r = 0$, and $m = nq$.

44. Write $m = n + k$, $k \ge 1$. We have

$$a^{2^{n+k}} - 1 = (a^{2^{n+k-1}} + 1)(a^{2^{n+k-1}} - 1),$$

so if $a^{2^n}+1$ divides $a^{2^{n+1}}-1$ ($k = 1$), and if it divides $a^{2^{n+k-1}}-1$, then it divides $a^{2^{n+k}}-1$. The result follows by induction. Now we have

$$a^{2^m} + 1 = a^{2^m} - 1 + 2 = (a^{2^n} + 1)y + 2$$

for some integer y. Therefore $(a^{2^m}+1, a^{2^n}+1)$ divides 2. If a is odd, $2 \mid a^{2^m}+1, a^{2^n}+1$, hence the greatest common divisor is 2. If a is even, $2 \nmid a^{2^m}+1, a^{2^n}+1$, hence the greatest common divisor is 1.

2. *(1 point.)* Let r be the largest integer such that $2^r \mid n$. Then $r \ge 0$ and $n = 2^r m$ where $2 \nmid m$, that is m is odd.

4.(a) *(2 points.)* Clearly p divides (a^2, b). If q is a prime dividing (a^2, b) then q divides a^2, b, hence a, b, hence $(a, b) = p$, so $q = p$. Hence (a^2, b) is a positive power of p. If p^3 divides (a^2, b) then p^2 divides a^2, b, contradicting $(a^2, b) = p$. Hence $(a^2, b) = p$ or p^2. Indeed both are possible, for example take $a = b = p$.

5. (a) *(2 points.)* Obviously (ab, p^5) is a power of p. Clearly p^3 divides (ab, p^5), for p divides a and p^2 divides b. If $p^4 \mid (ab, p^5)$ then $p^2 \mid a$ or $p^3 \mid b$, contradicting $(a, p^2) = p$ and $(b, p^4) = p^2$ respectively. Hence $(ab, p^5) = p^3$.

(b) *(2 points.)* Obviously $(a+b, p^4)$ is a power of p. We have $a = pa', b = p^2 b'$, where $p \nmid a', b'$. Then $a + b = p(a' + pb')$ and $p \nmid a' + pb'$, so p divides $a+b$ but p^2 does not. Hence $(a+b, p^4) = p$.

7. *(2 points.)* We have $ab = \prod_p p^{2\nu_p}$, and since $(a, b) = 1$, if $p \mid a$ then $p \nmid b$ and vice-versa. By uniqueness of factorization, we must then have $a = \prod_{p|a} p^{2\nu_p}$ and $b = \prod_{p|b} p^{2\nu_p}$ are squares.

8. *(2 points.)* $(n, n+1) = 1$ (for $(n+1)\cdot 1 - n \cdot 1 = 1$), so if $n(n+1)$ is a square then n and $n+1$ are squares by 7. But this is impossible for no two squares differ by 1, except for $(\pm 1)^2$ and 0^2. To see this, note that if $a^2 - b^2 = (a+b)(a-b) = 1$, then $a + b = a - b = \pm 1$.

Alternatively, note that if n is positive then $n^2 < n(n+1) < (n+1)^2$.

17 points, plus 3 points for a reasonable attempt at all questions = 20 points.