Elementary Number Theory.

Hints of Problems 2-3. *by Jonathan Tsai*

6.(a) Show that: $n | \prod_{k=0}^{n-1}(a+k), \forall a \in \mathbb{Z}, \forall n \in \mathbb{N}$.

$[Hints]$: (methods)

(1) Mathematical induction.

(2) Division Algorithm.

(3) $\binom{a+(n-1)}{n} \in \mathbb{N}$, $\forall a \geq 1$. For $a < -(n-1)$, use another expression of binomial.

6.(b) Show that $3 | a(2a^2+7), \forall a \in \mathbb{Z}$.

$[Hint]$: (steps)

(1) $a(2a^2+7) = a(2a^2-2+9) = 9a + 2a(a^2-1) = 9a + 2(a+1)a(a-1)$ and use **6.(a)** for $a \in \mathbb{N}$.

(2) Let $f(x) = x(2x^2+7)$, then $f(-a) = -f(a), \forall a \in \mathbb{N}$.

That is, $3 \mid f(-a) = -f(a), \forall a \in \mathbb{N}$ because $3 \mid f(a), \forall a \in \mathbb{N}$

(3) $3 \mid f(0)$.

13.(a) Prove: $\exists\ x, y \in \mathbb{Z}$ such that $ax + by = c \Leftrightarrow gcd(a, b) | c$.

Proof.

"$\Rightarrow$":

Case 1: If $a \neq 0$ and $b \neq 0$, use **Corollary(2.3)** then done.

Case 2:

If $a = 0$, then $c = by$ for some $y \in \mathbb{Z}$ and hence $gcd(a, b) = b \mid c$.

If $b = 0$, then $c = ax$ for some $x \in \mathbb{Z}$ and hence $gcd(a, b) = a \mid c$.

"$\Leftarrow$":

Case 1: $(a = 0$ or $b = 0)$

If $a = 0$, then $gcd(a, b) = b \mid c$. Let $c = kb$ for some $k \in \mathbb{Z}$.

$\Rightarrow \exists x, k \in \mathbb{Z}$ such that $c = kb = 0 + kb = ax + bk$.

If $b = 0$, similar as above.$(gcd(a, b) = a \mid c)$

Case 2: $(a \neq 0$ and $b \neq 0)$

Since $gcd(a, b) \mid c$, we can let $d = gcd(a, b)$ and let $c = Kd$ for some $K \in \mathbb{Z}$.

By **Theorem(2.3)**, $\exists\ x, y \in \mathbb{Z}$ such that $d = gcd(a, b) = ax + by$.

$\Rightarrow \exists\ X = Kx,\ Y = Ky \in \mathbb{Z}$ such that $aX + bY = Kd = c$. $\square$

13.(b) Prove that if $\exists\ x, y \in \mathbb{Z}$ such that $ax + by = gcd(a, b)$, then $gcd(x, y) = 1$.

Proof.
Let $d = gcd(a, b)$ and $a = a_1 d$, $b = b_1 d$ for some $a_1, b_1 \in \mathbb{Z}$.
Then by **Theorem(Corollary 1 of 2.4)**, $gcd(a_1, b_1) = gcd(a/d, b/d) = 1$.
$\because ax + by = d$, $\therefore a_1 dx + b_1 dy = d \Rightarrow a_1 x + b_1 y = 1$
Let $k = gcd(x, y)$, then $k \mid x$ and $k \mid y \Rightarrow k \mid (a_1 x + b_1 y) \Rightarrow k \mid 1 \Rightarrow k = \pm 1$.
Since $k = gcd(x, y) > 0$, $k = 1$. That is, $gcd(x, y) = 1$. □

20.
(a) Prove that $gcd(a, b) = 1$ and $gcd(a, c) = 1$ implies $gcd(a, bc) = 1$.
(b) Prove that if $gcd(a, b) = 1$ and $c|a$, then $gcd(b, c) = 1$.
(c) Prove that if $gcd(a, b) = 1$, then $gcd(ac, b) = gcd(c, b)$.

Proof.
(a)
$\because gcd(a, b) = gcd(a, c) = 1 \therefore$ by **Thm(2.3)**, $\exists\ p, q, r, s \in \mathbb{Z}$ s.t. $ap + bq = ar + cs = 1$.
$\Rightarrow (ap + bq)(ar + cs) = 1 \Rightarrow a(apr + pcs + bqr) + bc(qs) = 1$.
$\Rightarrow \exists X = (apr + pcs + bqr)$ and $Y = (qs)$ s.t. $aX + bcY = 1$
$\Rightarrow gcd(a, bc) = 1$ (by **Thm(2.4)**).
(b)
$\because gcd(a, b) = 1$, $\therefore$ by **Thm(2.3)**, $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = 1$.
$\because c \mid a$, $\therefore$ we can let $a = kc$ for some $k \in \mathbb{Z}$. Then $c(kx) + b(y) = 1$.
$\Rightarrow gcd(b, c) = 1$ (by **Thm(2.4)**).
(c)
If $c = 0$, then done.
If $c \neq 0$, let $gcd(ac, b) = d_1$ and $gcd(c, b) = d_2$. Then by **Thm(2.3)**:
$\exists\ x_1, y_1 \in \mathbb{Z}$ such that $ac(x_1) + b(y_1) = d_1$ and $\exists\ x_2, y_2 \in \mathbb{Z}$ such that $c(x_2) + b(y_2) = d_2$.
$\Rightarrow c(ax_1) + by_1 = d_1$ and $ac(x_2) + a(by_2) = ad_2$
$\Rightarrow d_2 \mid c$ and $d_2|b$ and $d_1 \mid ad_2$ (by **Cor(2.3)**)
$\Rightarrow d_2 \mid (c(ax_1) + b(y_1))$ (by **Thm(2.2)**) and $d_1 \mid d_2$ (since $gcd(a, d) = 1$)
$\Rightarrow d_2 \mid d_1$ and $d_1 \mid d_2 \Rightarrow d_1 = d_2 \Rightarrow gcd(ac, b) = gcd(c, b)$. □

21.(a) Prove that if $d|n$, then $(2^d - 1) \mid (2^n - 1)$.

Proof.
Let $n = kd$ for some $k \in \mathbb{Z}$.
$\because (x^r - 1) = (x - 1)(x^{r-1} + x^{r-2} + ... + x^2 + x + 1)$, $\forall r \in \mathbb{N}$
$\therefore (2^n - 1) = (2^{kd} - 1) = (2^d - 1)(2^{(k-1)d} + 2^{(k-2)d} + ... + 2^{2d} + 2^d + 1)$.(here $x = 2^d$ and $r = k$)
$\Rightarrow (2^d - 1) \mid (2^n - 1)$. □

Hints of Problems 2-4. *by Jonathan Tsai*

2. Euclidean Algorithm - please follow the process in the test book.

4.(b) Assume $gcd(a, b) = 1$, prove that $gcd(2a + b, a + 2b) = 1$ or 3

Proof.
Let $d = gcd(2a + b, a + 2b)$, then $d \mid (2a + b)$ and $d \mid (a + 2b)$
$\Rightarrow d \mid [2(2a + b) - (a + 2b)] = 3b$ and $d \mid [-(2a + b) + (a + 2b)] = 3a$
$\Rightarrow 0 < d \mid gcd(3a, 3b) = 3gcd(a, b) = 3$ (since $gcd(a, b) = 1$)
$\Rightarrow d = 1$ or 3.

$\square$

5.(a) Prove that if $gcd(a, b) = 1$, then $gcd(a^n, b^n) = 1, \forall a, b, n \in \mathbb{N}$.
[*Hint*] :
Use induction and **2-3.20.(a)** to prove $gcd(a, b^n) = 1$ and $gcd(a^n, b) = 1, \forall a, b, n \in \mathbb{N}$.
Then use induction to and **2-3.20.(a)** again to prove $gcd(a^n, b^n) = 1, \forall a, b, n \in \mathbb{N}$.

6. Prove that if $gcd(a, b) = 1$, then $gcd(a + b, ab) = 1$.

Proof.
Let $d_1 = gcd(a + b, a)$, then $d_1 \mid a$ and $d_1 \mid (a + b)$
$\Rightarrow d_1 \mid a$ and $d_1 \mid ((a + b) - a) = b$
$\Rightarrow d_1 \mid gcd(a, b) = 1 \Rightarrow d_1 = 1$ (since $d_1 > 0$).
On the other hand, let $d_1 = gcd(a + b, b)$. Then one can also obtain $d_2 = 1$.
Hence $gcd(a + b, a) = gcd(a + b, b) = 1$.
$\Rightarrow gcd(a + b, ab) = 1$ by **2-3.20.(a)**. $\square$

Problems 2-5. Linear Diophantine equation
Please follow the solving process in the textbook.
Theorem 2.9
The equation $ax + by = c$ (*) has a solution $\Leftrightarrow gcd(a, b) \mid c$
Moreover, if $(x, y) = (x_0, y_0)$ is a solution, then all the solutions of (*) are:
$(x, y) \in \{(x_0 + (\frac{b}{d})t, y_0 - (\frac{a}{d})t) \mid d = gcd(a, b),\ t \in \mathbb{Z}\}$.