SKETCH OF SOLUTIONS (HOMEWORK I)

Part I

2.
$$\begin{aligned}\gcd(2^4\cdot 3^2\cdot 5\cdot 7^2, 2\cdot 3^3\cdot 7\cdot 11) &= 2\cdot 3^2\cdot 7\\ \operatorname{lcm}(2^3\cdot 3^2\cdot 5, 2\cdot 3^3\cdot 7\cdot 11) &= 2^3\cdot 3^3\cdot 5\cdot 7\cdot 11\end{aligned}$$

4. $s=-3$, $t=2$. s and t are not unique: take $s=8$ $t=-5$

16.
$$\begin{aligned}126 &= 3(34)+24\\ 34 &= 1(24)+10\\ 24 &= 2(10)+4\\ 10 &= 2(4)+2\\ 4 &= 2(4)\end{aligned}$$

Using these equations we get:
$$2 = 26(34) - 7(126)$$

7. We may assume (*why?*) that $a = p_1^{\alpha_1}\cdots p_n^{\alpha_n}$ and $b = p_1^{\beta_1}\cdots p_n^{\beta_n}$ with $0\le \alpha_i,\beta_i$ then $\gcd(a,b) = p_1^{m_1}\cdots p_n^{m_n}$ and $\operatorname{lcm}(a,b) = p_1^{M_1}\cdots p_m^{M_n}$ where $m_i = \min\{\alpha_i,\beta_i\}$ and $M_i=\max\{\alpha_i,\beta_i\}$. Since $m_i+M_i=\alpha_i+\beta_i$ we get
$$ab = p_1^{\alpha_i+\beta_i}\cdots p_n^{\alpha_n+\beta_n} = p_1^{m_i+M_i}\cdots p_n^{m_n+M_n} = \operatorname{lcm}(a,b)\gcd(a,b)$$

Another proof that does not use the fundamental theorem of arithmetics. Set $d=\gcd(a,b)$ and let $a=a'd$ and $b=b'd$. Then $\gcd(a',b')=1$ (*why?*) and $\operatorname{lcm}(a',b') = a'b' = ab/d^2$ (*why?*). Then $\operatorname{lcm}(a,b) = \operatorname{lcm}(a'd,b'd) = d\operatorname{lcm}(a',b') = ab/d$.

8. Since $a\mid c$, $c=am$ for some $m\in\mathbb{Z}$, also, since $b\mid c$ and $b\nmid a$ (since $(a,b)=1$) we must have by Euclid's lemma that $b\mid m$ i.e. $m=bn$ therefore $c=abn$ so $ab\mid c$. Example when $\gcd(a,b)\ne 1$: $a=b=2$ and $c=6$.

14.
$$7(5n+3)-5(7n+4)=1 \therefore (5n+3,7n+4)=1$$

18. Suppose $p_1\cdots p_n+1 = p_i m$ for some $m\in\mathbb{Z}$, then
$$1 = p_i m - p_i(p_1\cdots p_{i-1}p_{i+1}\cdots p_n) = p_i(m-(p_1\cdots p_{i-1}p_{i+1}\cdots p_n)) \therefore p_i\mid 1$$
but this is impossible.

19. Suppose there are finitely many prime numbers and $p_1,\ldots,p_n$ is their complete list. Then, by exercise 18, $p_1\cdots p_n+1$ is not divisible by any of these primes. However, by the fundamental theorem of arithmetic it should be a represented as a product of these prime numbers — a contradiction.

26. By induction on n (using the second PMI)
Base: $f_1 = 1 < 2^1$
Inductive step: Suppose $f_n < 2^n$, $\forall n < N$ then $f_{N+1} = f_N + f_{N+1} < 2^N + 2^{N+1} < 2^N + 2^N = 2\cdot 2^N = 2^{N+1}$

Part II

13.- Suppose $d = 1$ then there exist $s, t \in \mathbb{Z}$ such that $as + nt = 1$ i.e. $nt = 1 - as$ i.e $1 \equiv as \mod n$ thus, s is a solution to $ax \equiv 1 \mod n$.

Suppose now $ax \equiv 1 \mod n$ has a solution s, then $as - 1 = nk$ for some $k \in \mathbb{Z}$ i.e. $as - nk = 1$ therefore $\gcd(a, n) = 1$

28. $n^3 - n = n(n^2 - 1) = n(n-1)(n+1) = (n-1)n(n+1)$. Since $n - 1$, n and $n + 1$ represent different cosets (mod 3) one of them must be the zero coset (mod 3). Hence $3|(n^3 - n)$. Also, one of these numbers must be even, hence $2|(n^3 - n)$. By exercise 8, since $\gcd(2, 3) = 1$, $6|(n^3 - n)$.

39. $a_{10} = 1$ it works since $(0, 6, 1, 8, 1, 2, 2, 1, 4, 1) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) = 154$ and $154 \equiv 0 \mod 11$

40. $x \equiv 7 \mod 11$

46. (1) $a \sim a$: True since $a - a = 0 \in \mathbb{Z}$
    (2) $a \sim b \Rightarrow b \sim a$: If $a - b \in \mathbb{Z}$ then $b - a = -(a - b) \in \mathbb{Z}$
    (3) $a \sim b, b \sim c \Rightarrow a \sim c$: If $a - b \in \mathbb{Z}$ and $b - c \in \mathbb{Z}$ then $(a - b) + (b - c) \in \mathbb{Z}$ i.e. $a - c \in \mathbb{Z}$

    The equivalence classes are given by sets of the form $r + \mathbb{Z}, r \in \mathbb{R}$

47. No, $-2 \sim 0$ and $2 \sim 0$ but $-2 \nsim 2$

48. (1) $a \sim a$: True since $a + a = 2a$ which is even
    (2) $a \sim b \Rightarrow b \sim a$: If $a + b = 2m$ then $b + a = 2m$
    (3) $a \sim b, b \sim c \Rightarrow a \sim c$: If $a + b = 2m$ and $b + c = 2k$ then $a + c = 2m - b + 2k - b = 2(m + k - b)$

    There are two equivalence classes:

    [0] = The set of all even integers.

    [1] = The set of all odd integers.