Solutions to selected problems in homeworks 1-5.

1.4. Let a and b be positive integers and $d = gcd(a, b)$.

(a) Prove that for any integer c such that $c > ab - a - b$ and $d \mid c$ there exist nonnegative integers x and y such that $c = ax + by$. **Hint:** Let x be the smallest nonnegative integer such that $c = ax + by$ for some $y \in \mathbb{Z}$ (explain why such x exists). Show that $x < b$ and deduce that y corresponding to this x is nonnegative.

(b) Assume that a and b are coprime, that is $d = 1$. Prove that $c = ab-a-b$ cannot be written as $c = ax+by$ where x and y are nonnegative integers.

(c) Now assume that a and b are NOT coprime. Prove that $c = ab - a - b$ can be written as $c = ax + by$ for nonnegative integers x and y.

Solution: (a) First of all note that $c > (a-1)(b-1) - 1 \geq -1$, so $c \geq 0$ (since c is an integer). Since $d \mid c$, we know that there exist some integers (not necessarily non-negative) x_0 and y_0 such that $ax_0 + by_0 = c$. Moreover,

$$\text{for any } k \in \mathbb{Z}, \quad x = x_0 - kb \text{ and } y = y_0 + ka \text{ also satisfy } ax + by = c. \tag{***}$$

Since $ax_0 + by_0 = c \geq 0$ and $a, b > 0$, at least one of the integers x_0 and y_0 is non-negative, and without loss of generality assume that $x_0 \geq 0$. Let

$$S = \{x \in \mathbb{Z}_{\geq 0} : ax + by = c \text{ for some } y \in \mathbb{Z}\}.$$

Then S is non-empty since $x_0 \in S$, and thus S has the smallest element, call it x (thus, by definition, $x \geq 0$). We claim that $x \leq b - 1$. Indeed, if $x \geq b$, then $x - b \geq 0$, whence by (***), $x - b \in S$, contradicting minimality of x.

Since $x \in S$, there exists $y \in \mathbb{Z}$ such that $ax + by = c$. Since $x < b$ and $c > ab - a - b$, we get $by = c - ax > ab - a - b - a(b-1) = -b$, and dividing by b we get $y > -1$. But y is an integer, so $y \geq 0$, so we found non-negative x and y for which $ax + by = c$.

(b) Observe that $c = ab-a-b = a(b-1)+b(-1)$, so $(x_0, y_0) = (b-1, -1)$ is a solution to the equation $ax + by = c$. Since $gcd(a, b) = 1$, by Theorem 1.13 in the book, any other solution (x, y) is given by $x = x_0 - bk = (b-1) - bk$ and $y = y_0 + ak = -1 + ak$ for some $k \in \mathbb{Z}$.

We claim that there is no way to make both x and y non-negative. Indeed, if $k \leq 0$, then $y = -1 + ak \leq -1 < 0$, and if $k > 0$, then $x = b - 1 - bk \leq b - 1 - b = -1 < 0$.

(c) This time by our assumption $d = gcd(a, b) \geq 2$ (so in particular, a and b are at least 2). As in (b), we see that for any $k \in \mathbb{Z}$, the pair $x = b - 1 - \frac{b}{d}k$ and $y = -1 + \frac{a}{d}k$ is a solution to $ax + by = n$. We claim that taking $k = 1$ will make both x and y non-negative. Indeed, for $k = 1$ we get $x = b - 1 - \frac{b}{d} \geq b - 1 - \frac{b}{2} = \frac{b}{2} - 1 \geq 0$ since $b \geq 2$. On the other hand, $a \geq d$, so $y = -1 + \frac{a}{d} \geq -1 + 1 \geq 0$.

3.6. The main goal of this problem was to show that the largest integer n with the property that $x^2 \equiv 1 \mod n$ for all x coprime to n is equal to 24. The suggested method of solution was rather cumbersome since at that point we did not have the ring-theoretic Chinese remainder theorem, which is a powerful tool for such problems. In fact, we will prove a stronger result (Theorem 1 below), which in particular implies parts (a),(c) and (e) of 3.6. Also note that Problem 3.6(b) is a special case of 5.7, but formulated in a different language.

Theorem: *Let S be the set of all integers $n \geq 1$ satisfying the following property: $x^2 \equiv 1 \mod n$ for any $x \in \mathbb{Z}$ such that $gcd(x, n) = 1$. Then $n \in S$ if and only if n divides 24.*

Proof: First, by a standard reduction, a positive integer n lies in $S \iff g^2 = e$ for all $g \in U_n$.

Now take any $n \geq 1$, and let $n = p_1^{a_1} \dots p_k^{a_k}$ be the prime factorization of n. Then $U_n \cong U_{p_1^{a_1}} \times \dots \times U_{p_k^{a_k}}$. Since group isomorphisms preserve orders of elements, $n \in S \iff g^2 = e$ for all $g \in U_{p_1^{a_1}} \times \dots \times U_{p_k^{a_k}}$.

Let $g = (g_1, \dots, g_k)$ be an arbitrary element of $U_{p_1^{a_1}} \times \dots \times U_{p_k^{a_k}}$. Then $g^2 = e \iff g_i^2 = e$ for all $1 \leq i \leq k$. Hence equality $g^2 = e$ holds identically in U_n if and only if it holds identically in $U_{p_i^{a_i}}$ for each i.

Combining the results of the first two paragraphs, we conclude that

$$n \in S \iff p_i^{a_i} \in S \text{ for each } i, \qquad (*)$$

so we are essentially reduced to the question of which prime powers lie in S.

If p is an odd prime, the group U_{p^a} is cyclic and thus contains an element of order $\phi(p^a) = p^{a-1}(p-1)$. Thus, equation $g^2 = e$ may hold identically in U_{p^a} only if $p^{a-1}(p-1) \leq 2$ which only happens for $p = 3$, $a = 1$.

If $p = 2$ and $a \geq 4$, the element $g = [5]_{2^a}$ clearly does not satisfy $g^2 = e$ (since $25 \not\equiv 1 \mod 16$), so the only positive powers of 2 which may be in S

are $2, 4, 8$.

By direct verification, one shows that $2, 3, 4$ and 8 do lie in S, and by the above argument these are the only prime powers which lie in S. Combining this with (*), we get that $n \in S$ if and only if all prime powers in its decomposition are equal to $2, 3, 4$ or 8, that is $n = 2^a \cdot 3^b$ where $a \leq 3$ and $b \leq 1$. Clearly this happens $\iff$ n divides $2^3 \cdot 3 = 24$.

4.4. Let p be a prime.

(a) Use Problem 3(d) and Corollary 7.5 from class to prove that the group $\mathbb{Z}_p^\times$ is cyclic. **Hint:** A group of order n is cyclic if and only if it contains an element of order n.

(b) Let $m \in \mathbb{Z}$. Prove that the following are equivalent:

(i) $a^m \equiv 1 \mod p$ for all a with $p \nmid a$;

(ii) $(p-1) \mid m$.

Solution: (a) Recall that for a finite group G we let $o_{max}(G) = \max\{o(g) : g \in G\}$. According to 4.3(d), when G is abelian, the equality $g^{o_{max}(G)} = e$ holds for all $g \in G$.

Now let $U_p = \mathbb{Z}_p^\times$ and let $a = o_{max}(U_p)$. Then equality $g^a = e$ holds for all $g \in U_p$, whence $x^a \equiv 1 \mod p$ for $x = 1, 2, \ldots, p-1$ (since $[x]_p \in U_p$ for all such x). Thus, the congruence $x^a \equiv 1 \mod p$ has at least $p-1$ solutions mod p. On the other hand, by Corollary 7.5, it can have at most a solutions mod p. Therefore, $o_{max}(U_p) = a \geq p - 1 = |U_p|$.

Since for any finite group G we have $o_{max}(G) \leq |G|$ and equality holds $\iff$ G is cyclic, we conclude that $o_{max}(U_p) = |U_p|$ and U_p is cyclic.

(b) The implication "(ii)$\Rightarrow$ (i)" follows directly from little Fermat's theorem: if $m = (p-1)k$ for some $k \in \mathbb{Z}$ and $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$ by little Fermat, and raising both sides to power k, we get $a^{(p-1)k} = a^m \equiv 1 \mod p$.

Now we prove "(i)$\Rightarrow$ (ii)" Suppose that $a^m \equiv 1 \mod p$ for all a with $p \nmid a$. Equivalently, $g^m = e$ for all $g \in U_p$. In particular, this holds for g which is a generator of U_p (which exists by part (a)). Then $o(g) = |U_p| = p - 1$, and by Problem 4.3(a), equality $g^m = e$ implies that $p - 1$ divides m, as desired.

5.4. In this question we investigate the following question: given $n \in \mathbb{N}$, how many solutions can the equation $\phi(x) = n$ have?

(a) Prove that for any $n \in \mathbb{N}$, the equation $\phi(x) = n$ has only finitely many solutions.

(b) Read about Fermat primes in Chapter 2. Let $F_n = 2^{2^n} + 1$ be the n^{th} Fermat number. It is easy to verify directly that F_n is prime for $0 \leq n \leq 4$, and it is known that F_n is composite for $5 \leq n \leq 32$. Use these facts to compute the number of solutions to the equation $\phi(x) = 2^{2013}$.

(c) Let $n = 2pq$ where p and q are distinct odd primes. Prove that the equation $\phi(x) = n$ has a solution if and only if at the least one of the following holds: $q = 2p + 1$, $p = 2q + 1$ or $2pq + 1$ is prime. Also prove that the number of solutions is equal to 0, 2 or 4.

Solution to (a) and (c): We start with a simple, but very useful lemma:

Lemma: *Let $n \geq 3$. Then $\phi(n)$ is even (in particular, $\phi(n) \geq 2$).*

Proof: If a prime factorization of n includes an odd prime p, then $\phi(n)$ is divisible by $p - 1$, hence even. If a prime factorization of n does not include an odd prime p, then $n = 2^a$ for some $a \geq 2$ (since $n \geq 3$), so $\phi(n) = 2^{a-1}$ is also even.

Solution to (a): Take any x such that $\phi(x) = n$, and let $x = p_1^{a_1} \dots p_k^{a_k}$ be a prime factorization of x (that is, $p_1, \dots, p_k$ are distinct primes and each $a_i > 0$). Then $\phi(x) = \phi(p_1^{a_1}) \dots \phi(p_k^{a_k})$. We will first bound each of the prime powers $p_i^{a_i}$ from above (by a function of n) and then bound the number of factors k. These would yield a bound for x in terms of n and imply that there are only finitely many x such that $\phi(x) = n$.

Since $\phi(x) \leq n$, we have $\phi(p_i^{a_i}) \leq n$ for each i. Since $\phi(p_i^{a_i}) = p_i^{a_i - 1}(p_i - 1)$, we have $p_i^{a_i - 1} \leq n$ and $p_i - 1 \leq n$. Therefore, $p_i \leq n + 1$, whence $p_i^{a_i} = p_i^{a_i - 1} \cdot p_i \leq n(n + 1)$.

By Lemma, $\phi(p_i^{a_i}) \geq 2$ unless $p_i^{a_i} = 2$, and since primes $p_1, \dots, p_k$ are distinct, there exists at most one i for which $p_i^{a_i} = 2$. Therefore, possibly with one exception, each of the factors $\phi(p_i^{a_i})$ contributes at least a factor of 2 in the factorization of $\phi(x)$, and thus $\phi(x) \geq 2^{k-1}$. Since $\phi(x) \leq n$, we get $k \geq 1 + \log_2(n)$.

Combining the two bounds, we get that $x = \prod_{i=1}^{k} p_i^{a_i} \leq (n(n+1))^{1+\log_2(n)}$. The latter expression is an explicit bound for the number of solutions of $\phi(x) = n$.

Solution to (c): Again let x be such that $\phi(x) = 2pq$, and let $x = p_1^{a_1} \dots p_k^{a_k}$ be a prime factorization of x. We first claim that there exists at most one i such that $p_i^{a_i} > 2$. Indeed, if there exist $i \neq j$ such that $p_i^{a_i} > 2$ and $p_j^{a_j} > 2$, then by Lemma $\phi(p_i^{a_i})$ and $\phi(p_j^{a_j})$ are both even, whence $\phi(x)$ is divisible by

4, a contradiction since $\phi(x) = 2pq$ and p and q are odd.

Thus, the only possibilities for x are $x = p_1^{a_1}$ or $x = 2p_1^{a_1}$ (and in the latter case p_1 is odd).

Case 1: $x = p_1^{a_1}$. If $a_1 \geq 3$, then $\phi(x)$ is divisible by p_1^2, a contradiction, so $x = p_1$ or p_1^2. If $x = p_1$, $\phi(x) = p_1 - 1$, so $x = 2pq + 1$. Moreover, $x = 2pq + 1$ is a solution if and only if $2pq+1$ is prime (since we assume that p_1 is prime).

If $x = p_1^2$, $\phi(x) = p_1(p_1 - 1)$. Since p_1 is prime, the equality $p_1(p_1 - 1) = 2pq$ holds if and only if one of the following holds:

(i) $p_1 = 2$ and $p_1 - 1 = pq$

(ii) $p_1 = p$ and $p_1 - 1 = 2q$

(iii) $p_1 = q$ and $p_1 - 1 = 2p$

Clearly, case (i) is impossible, case (ii) occurs if and only if $p = 2q + 1$ and (iii) occurs if and only if $q = 2p + 1$. It is also clear that (ii) and (iii) cannot hold simultaneously.

Overall, we get that the number of solutions of the form $x = p_1^{a_1}$ is equal to $0, 1$ or 2, and for any such solution p_1 is odd (as $p_1 = p, q$ or $2pq + 1$)

Case 2: $x = 2p_1^{a_1}$ with p_1 odd. Then $\phi(x) = \phi(2)\phi(p_1^{a_1}) = \phi(p_1^{a_1})$, so $\phi(2p_1^{a_1}) = n$ if and only if $\phi(p_1^{a_1}) = n$. Hence every solution found in case 1 yields the corresponding solution in case 2 (obtained by multiplication by 2), and there are no other solutions in case 2.

Thus, the total number of solutions is twice the number of solutions found in case 1, hence is equal to $0, 2$ or 4, and by the argument in case 1, solutions exist if and only if $p = 2q + 1$, $q = 2p + 1$ or $2pq + 1$ is prime.

5.7. Keeping the notations of Problem 4, assume that $R = \mathbb{Z}_n$ and $S = \mathbb{Z}_m$ where $m \mid n$, and $\phi : R \to S$ is defined by $\phi([x]_n) = [x]_m$ (we verified in class that such ϕ is well defined). Prove that

$$\phi(U_n) = U_m.$$

Hint: First consider the case when n is a prime power. In the general case write $n = p_1^{a_1} \dots p_k^{a_k}$ (where $p_1, \dots, p_k$ are distinct primes and each $a_i \geq 1$) and $m = p_1^{b_1} \dots p_k^{b_k}$ and consider the diagram

$$\begin{array}{ccc} U_n & \xrightarrow[f_1]{} & U_{p_1^{a_1}} \times \ldots \times U_{p_k^{a_k}} \\ {\scriptstyle f_3}\downarrow & & \downarrow{\scriptstyle f_4} \\ U_m & \xrightarrow{f_2} & U_{p_1^{b_1}} \times \ldots \times U_{p_k^{b_k}} \end{array} \tag{1}$$

where the maps f_1, f_2, f_3 and f_4 are defined by

$$f_1([x]_n) = ([x]_{p_1^{a_1}}, \ldots, [x]_{p_k^{a_k}})$$
$$f_2([x]_m) = ([x]_{p_1^{b_1}}, \ldots, [x]_{p_k^{b_k}})$$
$$f_3([x]_n) = [x]_m$$
$$f_4([x]_{p_1^{a_1}}, \ldots, [x]_{p_k^{a_k}}) = ([x]_{p_1^{b_1}}, \ldots, [x]_{p_k^{b_k}})$$

Note that this diagram is commutative, that is, $f_4 f_1 = f_2 f_3$ as maps. Use what you already know about f_1, f_2 and f_4 to prove that f_3 is surjective (which is what you need to show).

Solution: First let us emphasize that surjectivity of the map $f_3 : U_n \to U_m$ is not obvious. The map $[x]_n \mapsto [x]_m$ considered as a function from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ is clearly surjective. However, this does not immediately yield surjectivity of the map $f_3 : U_n \to U_m$ since it may happen that $gcd(x, m) = 1$ while $gcd(x, n) \neq 1$. In this case $[x]_m \in U_m$, but $[x]_n \notin U_n$, so there is no "obvious" element of U_n which maps to $[x]_m$.

However, the above problem does not arise if both n and m are powers of the same prime p. Indeed, if $n = p^a$ and $m = p^b$ (in this case $m \mid n \iff b \leq a$), then $gcd(x, n) = 1 \iff gcd(x, m) \iff p \nmid x$, so for any x such that $[x]_m \in U_m$, the element $[x]_n$ lies in U_n and hence the map f_3 is surjective in this special case.

Now we consider general case, using notations introduced in the hint. Note that $f_3 = f_2^{-1} f_4 f_1$ (where f_2^{-1} exists since f_2 is bijective). We know that composition of surjective maps is surjective and that f_2^{-1} and f_1 are bijective (hence surjective), so it remains to prove that f_4 is surjective.

From the definition of f_4 it is clear that f_4 is surjective $\iff$ for each $1 \leq i \leq k$, the map $f_{4,i} : U_{p_i^{a_i}} \to U_{p_i^{b_i}}$ given by $f_{4,i}([x]_{p_i^{a_i}}) = [x]_{p_i^{b_i}}$ is surjective. The latter is true by the special case considered above.