**1.** (§2.3, problem 17) Find all solutions to the congruence

$$x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}.$$

(Note that $x^3 - 9x^2 + 23x - 15 = (x-1)(x-3)(x-5)$.)

**Solution:** Given the factoring of the polynomial, we have the three solutions 1, 3, and 5 modulo 11 and the three solutions 1, 3, and 5 modulo 13. There should be 9 solutions to the congruence modulo 143.

Applying the Euclidean algorithm, we find that $6 \times 11 - 5 \times 13 = 1$, so that $\overline{11} \equiv 6 \pmod{13}$ and $\overline{13} \equiv 6 \pmod{11}$. Thus we can satisfy any system

$$\begin{aligned} x &\equiv a_1 \pmod{11} \\ x &\equiv a_2 \pmod{13} \end{aligned}$$

with the integer $x = 6 \times 13 \times a_1 + 6 \times 11 \times a_2$. We use this technique to fill in the table:

| | | (mod 11) 1 | 3 | 5 |
|---|---|---|---|---|
| | 1 | 144 | 300 | 456 |
| (mod 13) | 3 | 276 | 432 | 588 |
| | 5 | 408 | 564 | 720 |

Reducing these numbers modulo 143, we get the nine solutions

| | | (mod 11) 1 | 3 | 5 |
|---|---|---|---|---|
| | 1 | 1 | 14 | 27 |
| (mod 13) | 3 | 133 | 3 | 16 |
| | 5 | 122 | 135 | 5 |

**2.** (§2.3, problem 18) Given any positive integer $k$, prove that there are $k$ consecutive integers each divisible by a square greater than 1.

**Proof:** Given $k$, let $p_1, p_2, \ldots, p_k$ represent the first $k$ primes. Then $p_1^2, p_2^2, \ldots, p_k^2$ are relatively prime in pairs, so by the Chinese remainder theorem, we can find an integer

$x$ (determined modulo $p_1^2 \cdot p_2^2 \cdots p_k^2$) that satisfies the congruences

$$\begin{aligned} x &\equiv -1 \pmod{p_1^2} \\ x &\equiv -2 \pmod{p_2^2} \\ x &\equiv -3 \pmod{p_3^2} \\ &\vdots \\ x &\equiv -k \pmod{p_k^2}. \end{aligned}$$

Let $x$ be a solution to this system. Then for each $i = 1, \ldots, k$, we get $x + i \equiv 0 \pmod{p_i^2}$, so that $x + i$ is divisible by a square. The numbers $x, x+1, x+2, \ldots, x+k$ form the desired sequence. ∎

**3.** (§2.3, problem 20) Let $m_1$ and $m_2$ be arbitrary positive integers, and let $g = (m_1, m_2)$. Let $a_1$ and $a_2$ be arbitrary integers. Show that the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

has a solution if and only if $a_1 \equiv a_2 \pmod{g}$.

Show that if this condition is met, then the solution is unique modulo $[m_1, m_2]$. (That is, if $x_1$ and $x_2$ are solutions to the system, then $x_1 \equiv x_2 \pmod{[m_1, m_2]}$.)

**Proof:** Suppose first that we have an integer $x_0$ satisfying the two congruences. Then

$$x_0 = a_1 + rm_1 = a_2 + sm_2$$

for some integers $r$ and $s$, so that $a_1 - a_2 = sm_2 - rm_1$ is a linear combination of $m_1$ and $m_2$. Let $g = (m_1, m_2)$. By the proof of Theorem 1.3, we know that $g$ divides any linear combination of $m_1$ and $m_2$. Thus $g | a_1 - a_2$, so $a_1 \equiv a_2 \pmod{g}$.

Conversely, suppose $a_1 \equiv a_2 \pmod{g}$.

By the definition of congruence, we know that $a_1 + rm_1$ satisfies the congruence $x \equiv a_1 \pmod{m_1}$ for any integer $r$.

Now consider the congruence

$$a_1 + rm_1 \equiv a_2 \pmod{m_2}, \tag{1}$$

or $m_1 r \equiv a_2 - a_1 \pmod{m_2}$. We view $r$ as the unknown in this congruence.

Recall that $g = (m_1, m_2)$. Also, recall that we are assuming that $a_1 \equiv a_2 \pmod{g}$, which implies that $g | a_2 - a_1$.

Since $g | a_2 - a_1$, Theorem 2.17 says that there is a solution to congruence (1). Let $r_0$ be the a solution to (1), and set

$$x_0 = m_1 r_0 + a_1.$$

Then clearly $x_0 \equiv a_1 \pmod{m_1}$ and, since $r_0$ is a solution to (1), we have

$$x_0 \equiv m_1 r_0 + a_1 \equiv (a_2 - a_1) + a_1 \equiv a_2 \pmod{m_2}.$$

Thus $x_0$ is a solution to the original system of congruences.

To prove the second statement, assume that $x_1$ and $x_2$ are solutions to the given system. Then we have

$$\begin{aligned} x_1 - x_2 &\equiv a_1 - a_1 \equiv 0 \pmod{m_1} \\ x_1 - x_2 &\equiv a_2 - a_2 \equiv 0 \pmod{m_2} \end{aligned}$$

so that $x_1 - x_2$ is a common multiple of $m_1$ and $m_2$. By Theorem 1.12, we can conclude that $[m_1, m_2]$ divides $x_1 - x_2$, as required. ∎

**4.** Find all positive integers $x$ such that $\varphi(x) = 48$.

**Solution:** Here are some values of $\varphi(p^\alpha)$.

$$\begin{array}{llll} \varphi(2) = 1; & \varphi(2^2) = 2; & \varphi(2^3) = 4; & \varphi(2^4) = 8; \quad \varphi(2^5) = 16 \\ \varphi(3) = 2; & \varphi(3^2) = 6; & \varphi(3^3) = 18 & \\ \varphi(5) = 4; & \varphi(5^2) = 20 & & \\ \varphi(7) = 6 & & & \\ \varphi(11) = 10 & & & \\ \varphi(13) = 12 & & & \\ \varphi(17) = 16 & & & \\ \varphi(19) = 18 & & & \\ \varphi(23) = 22 & & & \end{array}$$

Next, for each factor $d$ of 48, we list the prime powers $p^\alpha$ such that $\varphi(p^\alpha) = d$.

| $d$ | prime powers |
|---|---|
| 1 | 2 |
| 2 | 3, 4 |
| 3 | |
| 4 | 5, 8 |
| 6 | 7, 9 |
| 8 | 16 |
| 12 | 13 |
| 16 | 17, 32 |
| 24 | |
| 48 | |

Next we consider all possible factorizations of 48 that might occur as products of the form

$$\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_1})\cdots\varphi(p_k^{\alpha_k}).$$

Write the factors in non-decreasing order.

Factorizations with smallest factor 2:

Factorizations starting $2 \times 2$: Since we can't have more than two 2's, any such factorization must be of the form $2 \times 2 \times 12$ or $2 \times 2 \times 3 \times 4$. The 3 can't occur, but we get

$$2 \times 2 \times 12 \;=\; \varphi(3)\varphi(4)\varphi(13).$$

Factorizations starting with $2 \times 3$: None of these can occur, because 3 does not occur as $\varphi$ of a prime power.

Factorizations starting with $2 \times 4$: Since 3 cannot occur, the only such factorization is $2 \times 4 \times 6$. This arises in several ways. We get

$$\begin{aligned} 2 \times 4 \times 6 &= \varphi(3)\varphi(5)\varphi(7) \\ &= \varphi(2)\varphi(3)\varphi(5)\varphi(7) \\ &= \varphi(3)\varphi(8)\varphi(7) \\ &= \varphi(4)\varphi(5)\varphi(7) \\ &= \varphi(4)\varphi(5)\varphi(9). \end{aligned}$$

Factorizations starting with $2 \times 6$: No non-decreasing factorizations begin this way. Same for $2 \times 8$ and $2 \times 12$.

The factorization $2 \times 24$ cannot occur, because 24 does not occur as $\varphi$ of any prime power.

Factorizations beginning with 3 may be ignored, because 3 does not occur as $\varphi$ of any prime power.

Factorizations beginning with 4: The only such factorization with non-decreasing factors is $4 \times 12$. This can arise in three ways:

$$\begin{aligned} 4 \times 12 &= \varphi(5)\varphi(13) \\ &= \varphi(2)\varphi(5)\varphi(13) \\ &= \varphi(8)\varphi(13) \end{aligned}$$

Factorizations beginning with 6: The only such factorization with non-decreasing factors is $6 \times 8$. This can arise in two ways:

$$\begin{aligned} 6 \times 8 &= \varphi(7) \times \varphi(16) \\ &= \varphi(9) \times \varphi(16). \end{aligned}$$

In order, the answers are

$$65,\ 104,\ 105,\ 112,\ 130,\ 140,\ 144,\ 156,\ 168,\ 180,\ 210.$$

**5.** (§2.3, problem 40) Prove that for $n \geq 2$ the sum of all positive integers less than $n$ and relatively prime to $n$ is $\dfrac{n\varphi(n)}{2}$.

**Proof:** Let $n \geq 2$ and let $R$ be the set of all positive integers less than $n$ and relatively prime to $n$. Then $|R| = \varphi(n)$. Furthermore, we claim that $k \in R$ if and only if $n - k \in R$.

For since $k \equiv n - k \pmod{n}$, by Theorem 2.4, $(k, n) = (n - k, n)$, so $k$ is relatively prime to $n$ if and only if $n - k$ is relatively prime to $n$. Also, $1 \leq k < n$ implies $n - 1 \geq n - k > 0$.

We also note that the mapping $k \mapsto n - k$ is a one-to-one correspondence of $R$ with itself.

Now let $S$ be the sum of the elements of $R$. Then

$$\begin{aligned} 2S &= 2\sum_{k\in R} k \\ &= \sum_{k\in R} k + \sum_{k\in R} n-k \\ &= \sum_{k\in R} k + n - k \\ &= \sum_{k\in R} n \\ &= n\varphi(n). \end{aligned}$$

Thus $S = \dfrac{n\varphi(n)}{2}$ as required. ∎