1. Let $a, b > 1$ be integers and $g := \gcd(a, b)$ its greatest common divisor. Show that if $a = g \cdot q_a$ and $b = g \cdot q_b$ then q_a and q_b are relatively prime.

   Solution. Since $\gcd(\kappa \cdot a, \kappa \cdot b) = \kappa \cdot \gcd(a, b)$ in particular, for $\kappa = g$ we have

$$g = \gcd(a, b) = \gcd(g \cdot q_a, g \cdot q_b) = g \cdot \gcd(q_a, q_b) \quad \Rightarrow \quad \gcd(q_a, q_b) = 1$$

   that is, q_a and q_b are relatively prime. □

---

2. Show that for any pair of non negative integers a and b

$$a \cdot b = \gcd(a, b) \cdot \mathrm{lcm}(a, b).$$

   Solution. Suppose first that a and b are relatively prime and let m be any multiple of both a and b. Then, for some integers q_a and q_b, $m = a \cdot q_a = b \cdot q_b$ and so, $a \mid b \cdot q_b$. Since a and b are relatively prime it follows that $a \mid q_b$, i.e., $q_b = \kappa \cdot a$ for some integer κ which implies that $m = a \cdot b \cdot \kappa$ and hence $a \cdot b \mid m$. This means that $a \cdot b$ being a multiple of a and b, is is a divisor of any its common multiples. Therefore, by the very definition of the least common multiple, it follows that $a \cdot b = \mathrm{lcm}(a, b)$.
   Finally, if a and b were not relatively prime, writing $a = g \cdot q_a$ and $b = g \cdot q_b$ as in exercise 1, since q_a and q_b are relatively prime we have for we just have proved

$$\begin{gathered} q_a \cdot q_b = \mathrm{lcm}(q_a, q_b) \\ \Downarrow \\ a \cdot b = (g \cdot q_a)(g \cdot q_b) \\ \Downarrow \\ a \cdot b = g^2 \cdot \mathrm{lcm}(q_a, q_b) \\ \Downarrow \\ a \cdot b = g \cdot \mathrm{lcm}(g \cdot q_a, g \cdot q_b) \\ \Downarrow \\ a \cdot b = g \cdot \mathrm{lcm}(a, b) \\ \Updownarrow \\ a \cdot b = \gcd(a, b) \cdot \mathrm{lcm}(a, b) \end{gathered}$$

   since as in exercise 1, $g = \gcd(a, b)$. □

---

3. Find gcd$(1000, 625)$

   (a) using the Euclidean Algorithm
   and

   (b) by factorization.

   Solution.

   (a) Successive divisions give the remainders

$$\begin{aligned} 1000 &= 625 \cdot 1 + 375 \\ 625 &= 375 \cdot 1 + 250 \\ 375 &= 250 \cdot 1 + 125 \\ 250 &= 125 \cdot 2. \end{aligned}$$

   This means that the last non zero reminder is 125 and hence

$$\gcd(1000, 625) = 125.$$

   (b) Since the prime factorizations of 1000 and 625 are

$$1000 = 2^3 \cdot 5^3$$

   and

$$625 = 5^4$$

   we find that $\gcd(1000, 625) = 2^0 \cdot 5^3 = 5^3 = 125.$ □

---

4. (a) If p is prime, show that the largest power of p dividing n! is

$$\sum_{j=1}^{\log_p n} \left\lfloor \frac{n}{p^j} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

   or

$$\frac{n - \sigma_p(n)}{p - 1}$$

   where $\sigma_p(n)$ denotes the sum of the base p digits of n.

   (b) 1000! has a lot of final zero digits. Use (a) to find how many are there.

Solution.

(a) There are

$$\#\left\{\kappa \;/\; 1 \leq \kappa, \text{ and } \kappa p \leq n\right\} = \#\left\{\kappa \;\Big/\; 1 \leq \kappa \leq \frac{n}{p}\right\} = \left\lfloor \frac{n}{p} \right\rfloor$$

multiples of p which are $\leq n$. In the same way, for $j = 1, 2, \ldots$ there are

$$\#\left\{\kappa \;/\; 1 \leq \kappa, \text{ and } \kappa p^j \leq n\right\} = \#\left\{\kappa \;\Big/\; 1 \leq \kappa \leq \frac{n}{p^j}\right\} = \left\lfloor \frac{n}{p^j} \right\rfloor$$

multiples of p^j which are $\leq n$. Therefore, the largest power of p that divides $n!$ is

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Note that this sum ends up as soon as $p^j > n$, i.e., when $j > \log_p n$.
Alternatively, if $n = a_m p^m + a_{m-1} p^{m-1} + \cdots + a_1 p + a_0$ is the base p expansion of n then, for any $j = 1, 2, \ldots, m$, we have

$$\frac{n}{p^j} = a_m p^{m-j} + a_{m-1} p^{m-j-1} + \cdots + a_{j+1} p + a_j + \frac{a_{j-1}}{p} + \cdots + \frac{a_1}{p^{j-1}} + \frac{a_0}{p^j},$$

but since $0 \leq a_i \leq p - 1$,

$$\begin{aligned}\frac{a_{j-1}}{p} + \cdots + \frac{a_1}{p^{j-1}} + \frac{a_0}{p^j} &\leq (p-1)\left(\frac{1}{p} + \cdots + \frac{1}{p^{j-1}} + \frac{1}{p^j}\right) \\ &= (p-1)\left(\frac{\frac{1}{p}\left(1 - \frac{1}{p^j}\right)}{1 - \frac{1}{p}}\right) = 1 - \frac{1}{p^j} < 1\end{aligned}$$

we see that

$$\left\lfloor \frac{n}{p^j} \right\rfloor = a_m p^{m-j} + a_{m-1} p^{m-j-1} + \cdots + a_{j+1} p + a_j$$

and hence

$$\begin{aligned}\sum_{j=1}^{m} \left\lfloor \frac{n}{p^j} \right\rfloor = \; & a_m p^{m-1} + a_{m-1} p^{m-2} + \cdots + a_2 p + a_1 \\ & + a_m p^{m-2} + a_{m-1} p^{m-3} + \cdots + a_3 p + a_2 \\ & \vdots \\ & + a_m p + a_{m-1} \\ & + a_m\end{aligned}$$

$$
\begin{aligned}
&= a_1 + a_2(1+p) + a_3(1+p+p^2) + \cdots + a_m\left(1+p+\cdots+p^{m-1}\right)\\
&= \frac{a_1(p-1) + a_2(p^2-1) + a_3(p^3-1) + \cdots + a_m(p^m-1)}{p-1}\\
&= \frac{\left(a_1p + a_2p^2 + a_3p^3 + \cdots + a_mp^m\right) - (a_1+a_2+a_3+\cdots+a_m)}{p-1}\\
&= \frac{n-\sigma_p(n)}{p-1}.
\end{aligned}
$$

(b) If $s_p(n)$ denotes either of the quantities appearing in part (a), the prime decomposition of $n!$ is

$$n! = \prod_{\substack{p\le n\\ p \text{ prime}}} p^{s_p(n)}.$$

Since the number of zeros at the end of $n!$ coincides with the largest power of $10 = 2\cdot 5$ dividing $n!$ and $s_5(n) < s_2(n)$ we see that the total of such zeros is $s_5(n)$. In particular, when $n = 1000$

$$
\begin{aligned}
s_5(1000) &= \left\lfloor\frac{1000}{5}\right\rfloor + \left\lfloor\frac{1000}{25}\right\rfloor + \left\lfloor\frac{1000}{125}\right\rfloor + \left\lfloor\frac{1000}{625}\right\rfloor\\
&= 200 + 40 + 8 + 1 = 249
\end{aligned}
$$

and 1000! ends with 249 zeros. □

---

5. (a) Given two non negative relatively prime integers a an b, show that if x_0, y_0 is a particular solution of the Diophantine equation $ax + by = m$ then, any other solution is of the form

$$\begin{cases} x = x_0 + b\kappa\\ y = y_0 - a\kappa\end{cases}$$

for some integer κ.

(b) Use (a) to describe the solution set for the general linear Diophantine equation $ax + by = m$ when a and b are arbitrary non negative integers.

Solution.

(a) If x_0, y_0 satisfies $ax_0 + by_0 = m$ and x, y is any other solution of this equation, i.e., $ax + by = m$, by subtracting

$$-a(x - x_0) = b(y - y_0).$$

This implies that $b \mid a(x - x_0)$ and hence $b \mid (x - x_0)$ because a and b are relatively prime. This means that for some integer κ, $x = x_0 + b\kappa$. Also, from the above relation it follows that $b(y - y_0) = -ab\kappa$ and so $y = y_0 - a\kappa$.

(b) Let x_0, y_0 be a solution of the general equation $ax + by = m$. We know that if $g: = \gcd(a, b)$ then, $g \mid m$ so if, as in exercise 1, we write $a = gq_a$ and $b = gq_b$, any solution x, y to the equation will satisfy

$$a_a x + q_b y = \frac{m}{g} \in \mathbb{Z}.$$

Since q_a and q_b are relatively prime (exercise 1), from part (a)

$$\begin{cases} x = x_0 + \kappa q_b \\ y = y_0 - \kappa q_a \end{cases}$$

for some integer κ.

---

6. Solve

$$\left.\begin{array}{l} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 5 \end{array}\right\}$$

Solution. From the first equation $x = 1 + 3\kappa$ and from the second $x = 2 + 5\ell$ form some integers κ and ℓ. This means that for x to be a solution of the given system, κ and ℓ must satisfy $1 + 3\kappa = 2 + 5\ell \Leftrightarrow 3\kappa = 1 + 5\ell$. Since 3 and 5 are relatively prime and $\kappa_0 = 2$, $\ell_0 = 1$ is a particular solution to this last equation, we see that its solutions are describe (exercise 5) by

$$\begin{cases} \kappa = 2 + 5\upsilon \\ \ell = 1 + 3\upsilon \end{cases}$$

where $\upsilon \in \mathbb{Z}$ is an arbitrary integer. Thus, returning to the expression for x in terms if κ (or ℓ) we find that the general solution to the given system of congruences is

$$x = 7 + 15\upsilon$$

with $\upsilon \in \mathbb{Z}$ an arbitrary integer.
In other words (recall the Chinese reminder theorem),

$$\left.\begin{array}{l} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 5 \end{array}\right\} \quad \Leftrightarrow \quad x \equiv 7 \mod 15.$$

□