Worksheet 3: Modular Arithmetic

1. Fix a positive integer m, and define the relation $x \sim y$ by $x \equiv y \bmod m$. Prove that $\sim$ is an equivalence relation.

2. Let $a, b, c, m \in \mathbb{Z}$ with $m > 0$.
   (a) Show that, if $\gcd(c, m) = 1$, then
   $$ac \equiv bc \pmod{m} \qquad \text{implies} \qquad a \equiv b \pmod{m}.$$
   (b) Give an example that shows that the gcd condition is necessary.

3. Suppose $a, b, m \in \mathbb{Z}$ with $m > 0$, and let $g := \gcd(a, m)$. Prove:
   (a) If $g \nmid b$ then $ax \equiv b \bmod m$ has no solution $x \in \mathbb{Z}$.
   (b) If $g \mid b$ then $ax \equiv b \bmod m$ has g distinct solutions x modulo m.
   (c) If $g = 1$ then a has a multiplicative inverse modulo m.

4. Suppose $a, m \in \mathbb{Z}$ with $m > 0$ and $\gcd(a, m) = 1$, and let $\{r_1, r_2, \dots, r_{\phi(m)}\}$ be a reduced residue system modulo m.
   (a) Show that $\{ar_1, ar_2, \dots, ar_{\phi(m)}\}$ is also a reduced residue system modulo m.
   (b) Conclude that $r_1 r_2 \cdots r_{\phi(m)} \equiv (ar_1)(ar_2) \cdots (ar_{\phi(m)}) \bmod m$ and, consequently, that
   $$a^{\phi(m)} \equiv 1 \pmod{m}.$$
   (This is *Euler's theorem*.)
   (c) Prove that, if p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \bmod p$. (This is *Fermat's little theorem*.)
   (d) Conclude that, if p is prime and $a, b \in \mathbb{Z}$, then $(a+b)^p \equiv a^p + b^p \bmod p$. (This is every freshman's dream.)

5. Suppose p is prime. Prove that $x^2 \equiv 1 \bmod p$ has precisely the two solutions $x \equiv \pm 1 \bmod p$.

6. Suppose $m \in \mathbb{Z}_{>0}$.
   (a) Show that, if $m > 4$ is not prime, then $(m-1)! \equiv 0 \bmod m$.
   (b) Now suppose m is prime. Show that if $a \not\equiv 0, \pm 1 \bmod m$ then there exists $b \not\equiv 0, \pm 1, a \bmod m$ such that $ab \equiv 1 \bmod m$.
   (c) Conclude *Wilson's theorem*: $(m-1)! \equiv -1 \bmod m$ if and only if m is prime.

7. Andrews 5.1.1–3, 3.2.3, 5.2.3, and 5.2.19.

8. Experiment with the `sage` command `mod`. Compare the running times of $2^{1000000000000} \bmod 3$ and $(2 \bmod 3)^{1000000000000}$. What do you think `sage` does?

9. Compute $7^{43} \bmod 11$ without `sage`. Check your answer with `sage`.

10. Write down a precise statement for each definition we have given this week. For each definition, give an example and a non-example.