PROBLEM-SOLVING AND PROOFS: ASSIGNMENT 8 SOLUTIONS

(1) *Variations on Wilsons Theorem.*

(a) Prove that if p is an odd prime, $2(p-3)!+1$ is divisible by p.

Solution: By Wilson's theorem we know $(p-1)! \equiv -1$, which we can write as

$$(p-3)!(p-2)(p-1) \equiv -1 \mod p.$$

But $(p-2)(p-1) \equiv (-2)(-1) \equiv 2 \mod p$ when $p > 2$, so this is exactly

$$2(p-3)! \equiv -1 \mod p$$

as desired.

(b) Prove that if p divides $(p-1)!+1$, then p is prime. (This is the converse to Wilsons Theorem.)

Solution: If p had a non-trivial factor $k \in \{2, 3, \ldots, p-1\}$, then by transitivity of divisiblity we would have $k \mid (p-1)!+1$; but k is one of the factors in the factorial $(p-1)!$ and thus $(p-1)!+1 \equiv 1 \not\equiv 0 \mod k$.

(2) *An important equivalence relation in analysis.* Fix a function $f : \mathbb{R} \to \mathbb{R}$, and let $O(f)$ denote the set of functions $g : \mathbb{R} \to \mathbb{R}$ for which there exist positive constants c and a such that $|g(x)| \leq c|f(x)|$ for all $x > a$. Now let S denote the set of all functions from $\mathbb{R}$ to $\mathbb{R}$, and define a relation R on S by setting $(g, h) \in R$ if and only if $g - h \in O(f)$. Prove that R is an equivalence relation.

Solution: To show R is reflexive we need to show $g - g \in O(f)$ for all g; i.e. $0 \in O(f)$. But $|0| \leq c|f(x)|$ regardless of c, f, x, so we are done.

To show R is symmetric, we need to show $g - h \in O(f)$ assuming $h - g \in O(f)$. This follows immediately from the fact $|g(x) - h(x)| = |h(x) - g(x)|$.

To show R is transitive, we let g, h, l be arbitrary functions such that $(g, h) \in R$ and $(h, l) \in R$ and show that $(g, l) \in R$. Our assumption means exactly that there exist positive constants c_1, c_2, a_1, a_2 such that

$$\begin{aligned} x > a_1 &\implies |g(x) - h(x)| \leq c_1|f(x)|, \\ x > a_2 &\implies |h(x) - l(x)| \leq c_2|f(x)|. \end{aligned}$$

When x is greater than both a_1 and a_2 we can use these along with the triangle inequality to conclude

$$|g(x) - l(x)| \leq |g(x) - h(x)| + |h(x) - l(x)| \leq c_1|f(x)| + c_2|f(x)|.$$

Thus choosing $a = \max(a_1, a_2)$ and $c = c_1 + c_2$ we have shown $g - l \in O(f)$.

(3) *Linear Equations in Modular Arithmetic.* Let $n \in N$, let $a, b \in \mathbb{Z}$, and set $d = \gcd(a, n)$. Prove that the equation

$$ax \equiv b \mod n$$

has a solution if and only if $d|b$. Furthermore, prove that when $d|b$, there are exactly d distinct congruence classes of solutions.

Solution: If there is a solution x to $ax \equiv b \mod n$ then there is some $k \in \mathbb{Z}$ such that $ax = b + kn$. Writing this as $b = ax - kn$, we see that the RHS is divisible by any common divisor of a and n, and thus $d \mid b$. Conversely, suppose $d = \gcd(a, n)$ divides b. The Euclidean algorithm provides us with a solution (y, k) of

$$ay + kn = d;$$

so multiplying by the integer b/d we get

$$a\left(y\frac{b}{d}\right) \equiv b \mod n;$$

i.e. $x = yb/d$ is a solution. In fact, we can add any multiple of the integer n/d to such an x and still have a solution, since $a(n/d) = n(a/d)$ and a/d is an integer; so we have a family of solutions

$$x_k = y\frac{b}{d} + k\frac{n}{d}.$$

We have $x_{k+d} \equiv x_k \mod n$, and conversely if $x_k \equiv x_l \mod n$ then $d \mid k - l$; so these solutions x_k form d distinct congruence classes mod n generated by the congruence classes of k mod d.

Finally, to show these are the only solutions, note that if x is the solution constructed above and z is some other solution then $n = d \mid a(x - z)$ and thus $n/d \mid x - z$; so z is one of the x_k.

(4) *Eulers Theorem.* This is a generalization of Fermats little theorem to nonprime moduli. Let $\phi(n)$ denote the number of integers less than n which are relatively prime to n. For example, $\phi(10) = 4$ since 1, 3, 7, 9 are relatively prime to 10. Prove that if $a \in Z$ is relatively prime to n, then

$$a^{\phi(n)} \equiv 1 \mod n$$

Hint: Consider the set $\{ia : 1 \leq i \leq n-1, \gcd(i, n) = 1\}$ and mimic our proof of Fermats Little Theorem.

Solution: Consider the subsets

$$\mathbb{Z}_n^\times = \{\bar{i} : 1 \leq i \leq n-1, \gcd(i, n) = 1\}$$

and

$$X = \{i\bar{a} : i \in \mathbb{Z}_n^\times\}$$

of $\mathbb{Z}_n$. Note that if i and a are both relatively prime to n, then so is ia; and if $ia \equiv ja$ mod n then we can multiply by $a^{-1} \mod n$ (which exists because $\gcd(a, n) = 1$) to get $i \equiv j \mod n$. Thus the products ia are all distinct mod n, so their reductions mod n are distinct elements of $\mathbb{Z}_n^\times$, which implies $X = \mathbb{Z}_n^\times$.

Thus the product of the elements of $\mathbb{Z}_n^\times$ is the product of the elements of X; but we can factor out the as from the latter, which yields

$$\prod_{i \in \mathbb{Z}_n^\times} i \equiv \prod_{i \in X} i \equiv \prod_{i \in \mathbb{Z}_n^\times} ia \equiv a^{|Z_n^\times|} \prod_{i \in \mathbb{Z}_n^\times} i \mod n.$$

Since each element $i \in \mathbb{Z}_n^\times$ has a multiplicative inverse mod n, we can multiply both sides of this congruence by each of these inverses, yielding

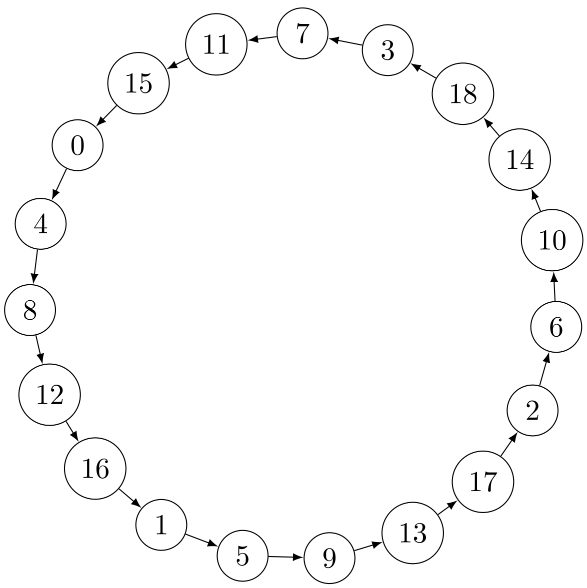
$$a^{|\mathbb{Z}_n^\times|} \equiv 1 \mod n.$$

Since $\phi(n)$ is defined exactly as the number of elements of $\mathbb{Z}_n^\times$, we have proved Euler's theorem.

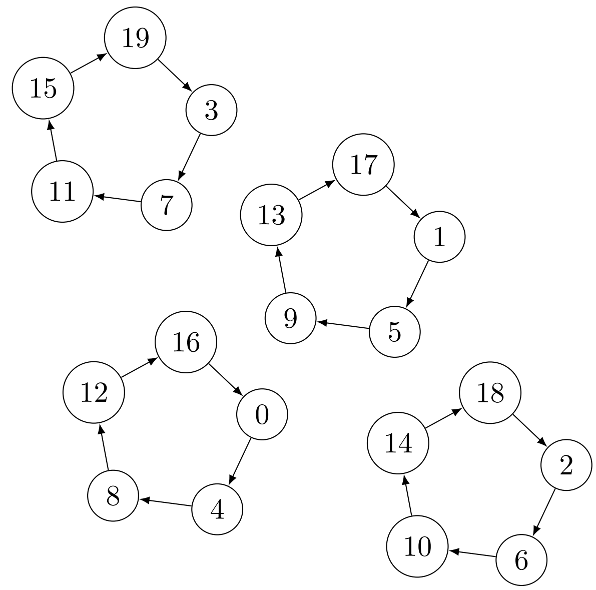
(5) *Functional Digraphs from Modular Arithmetic.* Define f and g from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ by

$$f(x) = x + a \mod n$$
$$g(x) = ax \mod n$$

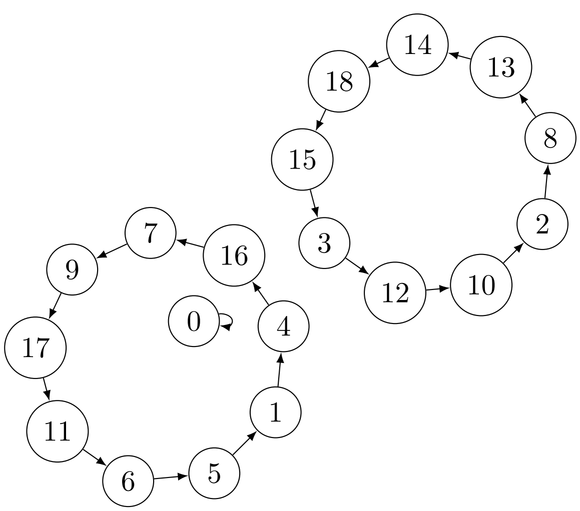
(a) Draw the functional digraphs of f and g in the cases $(n, a) = (19, 4)$ and $(n, a) = (20, 4)$.



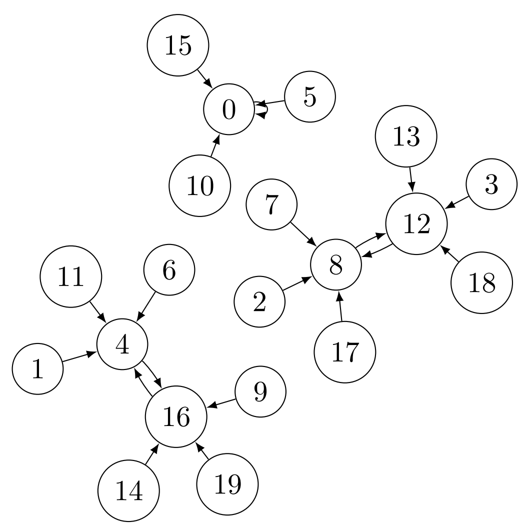
(A) $f : x \mapsto x + 4 \mod 19$



(B) $f : x \mapsto x + 4 \mod 20$



(A) $g : x \mapsto 4x \mod 19$



(B) $g : x \mapsto 4x \mod 20$

(b) Give a complete description of the functional digraph of f in terms of a and n.

Solution: Since $f(x) \equiv x + a$ has inverse $f^{-1}(x) \equiv x - a$, the functional digraph of f always consists entirely of cycles, since the incoming and outgoing degree of each vertex must be exactly one. The length of the cycle containing x_0 is the smallest k such that k consecutive applications of f bring x_0 back to itself; i.e. such that

$$x_0 + ka \equiv x_0 \mod n.$$

This is the smallest k such that $n \mid ka$, which is $n/\gcd(n,a)$.
Thus the functional digraph of f consists entirely of cycles of length $n/\gcd(n,a)$; so (since there are n vertices in total) there must be $\gcd(n,a)$ such cycles.

(c) Describe a property of the digraph of g which is true whenever n is prime and false whenever n is not a prime.

Solution: Answers vary - here's some discussion:
We saw in **5a** that the digraph of g for $(n,a) = (19,4)$ consists entirely of cycles with length dividing $n-1$. This is the case whenever n is prime and $a \not\equiv 0 \mod n$: by FLT we have

$$f^{n-1}(x) = a^{n-1}x \equiv x \mod n,$$

so we always get back to where we started by following $n-1$ consective arrows. However, this is not unique to prime n: for example, $(n,a) = (9,8)$ produces a very similar digraph to $(7,6)$.