Change log:

- Problem 4 (version 2): fixed wording.
- Problem 9 (version 2): emphasized reductions are required in both directions.

This problem set has a total of 10 written problems, plus 1 coding problem, on 2 pages. Written solutions should be submitted to Canvas by 2pm Wednesday Feb 10, 2020. Coding solutions can be submitted separately.

- If you find the sources of these problems, a citation of the source is sufficient for full points.
- If you choose not to submit a typed write-up, please write neat and legibly.

1. Show that if $6n+1$, $12n+1$, and $18n+1$ are all prime, than their product, $(6n+1)(12n+1)(18n+1)$ is a Carmichael number.

**SOLUTION:**
Let $p_1 = 6n+1, p_2 = 12n+1, p_3 = 18n+1$, then we want to show that $c = p_1p_2p_3$ is a Carmichael number. By the definition of Carmichael, for all integers $b$ such that $(b,c) = 1$, we want:

$$b^{c-1} \equiv 1 \pmod{c}$$

By CRT, this is equivalent to showing that the following holds:

$$b^{c-1} \equiv 1 \pmod{p_1}$$
$$b^{c-1} \equiv 1 \pmod{p_2}$$
$$b^{c-1} \equiv 1 \pmod{p_3}$$

The condition $(b,c) = 1$ implies that $(b, p_i) = 1$ for $i = 1, 2, 3$. So by Fermat’s Little Theorem, we have that $b^{p_i-1} \equiv 1 \pmod{p_i}$. So in order for $c$ to be a Carmichael number, we need that $c - 1 \equiv 0 \pmod{p_i - 1}$ for $i = 1, 2, 3$. We can finally take advantage of the convenient forms given for the primes $p_1, p_2, p_3$:

$$c = p_1p_2p_3 = (6n+1)(12n+1)(18n+1) = 1296n^3 + 396n^2 + 36n + 1 = 36n(36n^2 + 11n + 1) + 1$$

Hence, we have that $c - 1 \equiv 0 \pmod{p_i - 1}$ for $i = 1, 2, 3$. 

1
2. Consider the sequence

\[
\begin{align*}
a_0 &= 2 \\
a_1 &= 1 \\
a_n &= a_{n-1} + a_{n-2}
\end{align*}
\]

Show that if \( n \) is prime, then \( a_n \equiv 1 \pmod{n} \).

Recall the totient function \( \phi(n) \) for an integer \( n \) with prime factorization

\[
n = \prod p_i^{e_i}
\]

is

\[
\phi(n) = \prod (p_i - 1)p_i^{e_i-1}.
\]

**SOLUTION:**

**METHOD 1:** This sequence reminds us of the Fibonacci sequence, only the initial two terms are different. So then we can still apply the same techniques from Fibonacci to determine the closed form of \( a_n \), which tells us that:

\[
a_n = \left( \frac{1 + \sqrt{5}}{2} \right)^n + \left( \frac{1 - \sqrt{5}}{2} \right)^n
\]

We can easily confirm the \( n = 2 \) case, so assume \( n \) is an odd prime. Then

\[
a_n = \sum_{k=0}^{(n-1)/2} \binom{n}{2k} 5^k
\]

By Fermat’s Little Theorem, we have that \( (2^{-1})^{n-1} \equiv 1 \pmod{n} \). In the numerator, we have that \( \binom{n}{2k} \equiv 0 \pmod{n} \) for \( k > 0 \) since \( n \) is prime. Thus,

\[
a_n \equiv \sum_{k=0}^{(n-1)/2} \binom{n}{2k} 5^k \equiv \sum_{k=0}^{(n-1)/2} \binom{n}{2k} 5^k \equiv \binom{n}{0} 5^0 \equiv 1 \pmod{n}
\]

**METHOD 2:** Notice that this sequence is called the Lucas numbers. We proceed with a combinatorial argument. The Lucas number \( a_n \) counts the number of ways to construct a circular bracelet of length \( n \), constructed of beads of length 1 and length 2, where bracelets that are symmetric with respect to rotation or reflection are considered distinct.

As \( a_n = a_{n-1} + a_{n-2} \), we notice that we add a bead of length 1 to \( a_{n-1} \) bracelets length \( n - 1 \) and a bead of length 2 to \( a_{n-2} \) bracelets length \( n - 2 \).
Now consider a prime length $n$. When a bracelet is not made up of a pattern of beads (ie: $12|12|12|12$), each of the $n$ rotations of a bracelet is unique. Except for the bracelet constructed of solely length 1 beads, no bracelet can be formed with a pattern for a prime $n$ as $n$ has no divisors. Thus, we have $a_n = kn + 1$, where $k$ are the bracelets formed when rotations are not unique. We see that $a_n \equiv 1 \pmod{p}$.

3. Show that we can check in (possibly randomized) polynomial time (in the number of digits of $n$) whether $\phi(n)$ is a power of 2.

**SOLUTION:**
Observe that in order for $\phi(n)$ to be a power of 2, $n = 2^k \cdot p_1 \cdot p_2 \ldots$, where all $p_i$ must be of the form $2^a + 1$.

These primes are called Fermat numbers, and it is easy to prove that they are of the form $2^{2^b} + 1$. Consider an arbitrary $n = 2^{2j} + 1$, where $j$ is some odd number. We note that numbers of this form are divisible by $c = 2^a + 1$ as

$$n = (2^{2^a})^j + 1 = (c - 1)^j + 1 = g(c) \cdot c - 1 + 1 = g(c) \cdot c$$

where $g(C)$ is found after binomial expansion and $j$ is odd. Thus, $n = 2^{2j} + 1$ is prime only if $j = 1$, meaning $n$ has to be a Fermat prime. As of 2021, there are only 5 Fermat primes. Thus, we can divide $n$ by these 5 primes and check if the result is a power of 2 in polynomial time.

Note that Fermat primes grow at a fast enough rate that we are able to check even unconfirmed ones in polynomial time.

4. Show that if we can compute $\phi(n)$ for any $n$, we are able to factor semi-primes (numbers of the form $pq$ where $p$ and $q$ are both prime).

**SOLUTION:**
Note that $\phi(n) = (p - 1)(q - 1) = pq - p - q + 1$. We can subtract 1 and $n$ from $\phi(n)$ to recover $-p - q$.

Note that we are then left with a quadratic equation which we can use to find the factors of $n$.

For the next three problems, recall that $n$ is a pseudoprime to base $b$ when $b^{n-1} \equiv 1 \pmod{n}$.

5. Let $p$ be a prime $> 3$. Show that $\frac{2^{2p-1}}{3}$ is a pseudoprime to the base 2.

**SOLUTION:**
By definition of pseudoprime, we want to show that

$$2^{\frac{2^p-1}{3}} - 1 \equiv 0 \pmod{\frac{2^{2p}-1}{3}}$$

3
We can try to show a slightly stronger statement instead where we get rid of the fraction in the mod:

\[
2^{\frac{2^p-1}{3}} - 1 \equiv 0 \mod (2^{2p} - 1)
\]

Now note that \(2^a - 1\mid 2^b - 1 \iff a \mid b\). Hence, we need to show that \(2p\mid \frac{2^{2p-1}}{3} - 1\). We have that:

\[
\frac{2^{2p} - 1}{3} - 1 = \frac{2^{2p} - 4}{3} = \frac{2^{2p-2} - 1}{3} = 4 \cdot \frac{(2^{p-1} - 1)(2^{p-1} + 1)}{3}
\]

By Fermat’s Little Theorem, \(2^{p-1} - 1 \equiv 0 \mod p\), Hence \(2p\mid \frac{2^{2p-1}}{3} - 1\) as desired.

6. Let \(n\) be a pseudoprime to the base 2, show that \(2^n - 1\) is also a pseudoprime to the base 2.

**SOLUTION:**
By definition of pseudoprime, we have that \(2^n - 1 \equiv 1 \mod n\). We want to show that \(2^{2^n - 2} \equiv 1 \mod 2^n - 1\). Notice that the exponent \(2^n - 2\) can be rewritten in the following form:

\[
2^n - 2 = 2(2^{n-1} - 1) = 2kn
\]

for some integer \(k\) since \(2^{n-1} - 1 \equiv 0 \mod n\). Plugging this back in the desired equation, we need to show that

\[
2^{2kn} - 1 \equiv 0 \mod 2^n - 1
\]

And this is true because \(2^n - 1\) divides \((2^n)^{2k} - 1\).

7. Find a number that is a strong pseudoprime for the set of bases

\[B = \{ x \mid 2 \leq x \leq 31 \text{ and } x \text{ is prime}\}.
\]

**SOLUTION:**
Some examples are:

(a) 252601
(b) 3825123056546413051
(c) 1955097530374556503981

Refer to the following link:
8. Show that for any prime number \( p \), at least one of \(-1, 2, \) and \(-2\) is a square modulo \( p \).

**SOLUTION:**
Consider a generator of \( p \), \( g \). If \(-1\) is not a quadratic residue mod \( p \), then \( g^i \equiv -1 \) (mod \( p \)) for some odd \( i \). Similarly, if 2 is not a quadratic residue mod \( p \), then \( g^j \equiv 2 \) (mod \( p \)) for some odd \( j \). Then we have

\[ g^i \cdot g^j = g^{i+j} \equiv -2 \pmod{p} \]

which must be a quadratic residue as \( i + j \) must then be even. Thus, either \(-1, 2, \) or \(-2\) is a quadratic residue mod \( p \).

9. Show that computing the order for some \( a \) mod some \( n = pq \), with \( p \) and \( q \) hidden, but \( n \) given, is (randomized) poly-reducible to and from factoring \( n \). Note that you need to give reductions in both directions.

**SOLUTION:**
We first show that Order is poly-reducible to Factorization. Notice that by the Euler’s theorem, \( a^{\phi(n)} \equiv 1 \pmod{n} \). With the prime factorization of \( n \), it is easy to compute the terms of \( \phi(n) \).

Since the order of \( a \) must then divide \( \phi(n) \), We can incrementally check the terms of \( b = \phi(n) \) by taking \( a^{b/d} \pmod{n} \) for some term \( d|\phi(n) \), replacing \( b \rightarrow b/d \) if \( d|b \). Note that this can be done in polynomial time.

We then show that Factorization is poly-reducible to Order. Refer to this reduction given within Shor’s Factoring Algorithm:


10. (continue from Pset 3 Problem 8) Show that for some value \( n, y \leq n^{10} \), prime \( p \in (10n, n^2) \) with \( p = 2^k \cdot 3 + 1 \), coefficients \( a, b, \) and \( c \), we can compute the first \( n \) terms of the generating function

\[ \prod_{i=1}^{y} (1 - (ai^2 + bi + c) x) \pmod{p} \]

in \( \tilde{O}(n) \) time.

**SOLUTION:**
It suffices to sum the logs of these. Taylor expansion of log gives

\[ \ln (1 - (ai^2 + bi + c) x) = \sum_{j=1}^{\infty} -\frac{1}{j} (ai^2 + bi + c)^{j} x^{j}. \]
So it suffices to compute, for each $1 \leq j \leq n$,

$$\sum_{i=1}^{y} (a_i^2 + b_i + c)^j$$

If $a = b = 0$, this is just computing $c(c^y - 1)/(c - 1) \pmod{p}$, which is one fast exponentiation.

If $a = 0$, $b \neq 0$, we divide out $b^j$ to get to the $b = 1$ case, aka

$$\sum_{i=1}^{y} (i + c)^j = \sum_{i=c+1}^{y+c} i^j, \tag{1}$$

which is once again a term from the geometric series.

If $a \geq 0$, dividing out by $a^j$, and factoring out the square gives we’re computing

$$\sum_{i=1}^{y} ((i + c_1)^2 + c_2)^j = \sum_{i=1}^{y} \cdot \sum_{0 \leq k \leq j} \frac{j!}{k!(j-k)!} (i + c_1)^{2k} \cdot c_2^{j-k} \tag{2}$$

Pulling out the $j$ to the outside, and grouping the summation over $I$ with the $(i + c_1)^{2k}$ terms gives we’re computing, for each $j$,

$$j! \cdot \sum_{0 \leq k \leq j} \left( \frac{c_2^{j-k}}{(j-k)!} \right) \cdot \left( \frac{1}{k!} \sum_{i=1}^{y} (i + c_1)^{2k} \right). \tag{3}$$

This is once again a convolution: we can compute both of these series separately in $\tilde{O}(n)$ time.

**CODE** Separate submission on Canvas, 5 points.

This problem has a rather spooky and long story that essentially boils down to the following:

given $n \leq 80$ length 4 bitmasks,

$$0 \leq \text{mask}[1] \ldots \text{mask}[n] \leq 15.$$

We want to label these $n$ numbers by $0 \ldots 4$. A valid labeling is one where for all indices with the same digit sum, at least half of them are labeled same. For example, if $n = 80$, the numbers with digit sum 12:

$$\{39, 48, 57, 66, 75\}$$

have to have at least 3 labeled the same.

The result of each assignment is a length $5 \times 4$ bit vector formed by taking XOR fo all the masks assigned to that group. Find for each $2^{5 \times 4} = 2^{20}$ possible results, the number of assignments that lead to it, modulo $998244353 = 119 \times 2^{23} + 1$.

Autojudge: [https://dmoj.ca/problem/wac2p6](https://dmoj.ca/problem/wac2p6)