0: 11 Modom

We say an integer is *palindromic* if the digits read the same when written forward or backward. Prove that every palindromic integer with an even number of digits is divisible by 11.

Lemma: A number $n \in \mathbb{Z}$ is divisible by 11 if the alternating sum of the digits is divisible by 11.

Proof. We prove the lemma as follows. Let $n = a_k a_{k-1} a_{k-2} \dots a_1 a_0$ and the a_i are base ten digits. As such, $n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10a_1 + a_0$. Note that $10 \equiv -1(\mod 11)$. As such, we can say that

$$10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10a_1 + a_0 \mod 11 \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots - a_1 + a_0 \mod 11$$

The right part of the mod congruence is the alternating sum of n which is what we wanted. As such, the remainder of $\frac{n}{11}$ is equal to the remainder of $\frac{\text{alternating sum}}{11}$. Thus the lemma is true. □

We now go to the original statement. An arbitrary palindromic integer with an even number of digits l can be written as $l = a_0 a_1 a_2 a_3 a_4 \cdots a_n a_n \cdots a_4 a_3 a_2 a_1 a_0$ and the a_i are base ten digits. Applying our lemma, we know that $l \equiv 0 \mod 11$ when the alternating sum is divisible by 11. As such, we look at our alternating sum S which is formulated as follows:

$$S = a_0 - a_1 + a_2 - a_3 + a_4 - \cdots \pm a_n \mp a_n \cdots - a_4 + a_3 - a_2 + a_1 - a_0 \quad \text{[alternating sum]}$$
$$S = (a_0 - a_0) + (-a_1 + a_1) + (a_2 - a_2) + (-a_3 + a_3) + (a_4 - a_4) + \cdots + (\pm a_n \mp a_n)$$
$$S = 0$$
$$11|0 \quad \text{[by definition of |]}$$
$$11|S$$

As such, since the alternating sum S is divisible by 11, we can say that l is divisible by 11, and since l is an arbitrary palindormic integer with even digits, we have proven the original statement.

□

1: Too Many Twos

(a) Let x be an arbitrary n bits two's complement representation. As such, $x = b_{n-1}b_{n-2}\dots b_1b_0$ and $V(x) = -b_{n-1}2^{n-1} + \sum_{i=1}^{n-2} b_i 2^i$. We define a bit flipping function $f(b)$ as $f(b) = 1 - b$.

$$\begin{aligned}
V_{flip}(x) &= -f(b_{n-1})2^{n-1} + \sum_{i=1}^{n-2} f(b_i)2^i \\
&= (b_{n-1} - 1)2^{n-1} + \sum_{i=1}^{n-2} (1 - b_i)2^i \\
&= b_{n-1}2^{n-1} - 2^{n-1} + \sum_{i=1}^{n-2} 2^i - \sum_{i=1}^{n-2} b_i 2^i \\
&= b_{n-1}2^{n-1} - 2^{n-1} - \sum_{i=1}^{n-2} b_i 2^i + 2^{n-1} - 1 \qquad \text{[by finite geometric series theorem]} \\
V_{flip}(x) + 1 &= b_{n-1}2^{n-1} - \sum_{i=1}^{n-2} b_i 2^i - 1 + 1 \\
V_{flip}(x) + 1 &= -1 * (-b_{n-1}2^{n-1} + \sum_{i=1}^{n-2} b_i 2^i) \\
V_{flip}(x) + 1 &= -V(x)
\end{aligned}$$

As such, since x was arbitrary, we have shown that any fixed width two's complement representation with n bits can be negated by flipping all bits and adding 1.

(b) Since in the previous part we proved that the negation in two's complement is equivalent to negation over the integers, we can prove that negation in two's complement is bijective by proving the bijectivity of negation over the integers i.e. we have to prove the bijectivity of $f(x) = -x$. To prove bijectivity, we have to prove injectivity and surjectivity.

To prove injectivity, we assume that for all $x, y \in \mathbb{Z}$ $f(x) = f(y)$. Since $f(x) = f(y)$, $-x = -y$ which implies that $x = y$. As such, since $f(x) = f(y) \Rightarrow x = y$, f is injective.

To prove surjectivity, we let y be an arbitrary element in the integers such that $-2^{n-1} < y < 2^{n-1}$. We claim that $f(-y) = y$ and claim that $-y$ is in the domain since $-y \in \mathbb{Z}$ and

$$\begin{aligned}
-2^{n-1} &< y < 2^{n-1} \\
-1 * (-2^{n-1}) &< -y < -1 * 2^{n-1} \\
2^{n-1} &> -y > -2^{n-1}
\end{aligned}$$

so $-y$ is in the domain. As such, f is surjective. Since we have proven surjectivity and injectivity, we have shown f is bijective. As such negation of -2^{n-1} in two's complements is bijective.

2: OMgcd

(a) Let n and m be arbitrary positive integers with $n \leq m$. Prove that $m \mod n \leq \frac{m}{2}$.

We start be defining r to the be the result of $m \mod n$ such that $m \mod n = r$. We now rewrite m as follows:

$$\begin{aligned}
m \mod n &= r \\
m \mod n = r \mod n & \\
m \equiv_n r & \quad \text{[relation between mod and congruences]} \\
n|(m-r) & \quad \text{[definition of } \equiv_n\text{]} \\
m = nk + r & \quad \text{[definition of } | \text{ for some } k \in \mathbb{Z}\text{]}
\end{aligned}$$

From the above statement in combination with $n \leq m$, we know that $r < n$ and can perform the following calculations:

$$\begin{aligned}
r &< n \\
r + r &< n + r \\
r &< \frac{n+r}{2} \\
r < \frac{n+r}{2} \leq \frac{kn+r}{2} &= \frac{m}{2} \\
r &\leq \frac{m}{2} \\
m \mod n &\leq \frac{m}{2}
\end{aligned}$$

We have thus proven our original statement. □

(b) Assume $n \leq m$. Use part (a) to show that the Euclidean Algorithm will make a total of at most $2\log_2 m$ recursive calls.

We prove this by tracing out the recursive calls and assuming the worst case for each bound/parameter. The first call is `gcd(m, n)`. Since $n \neq 0$, the first recursive call is `gcd(m, m % n)`. From part a, we know that the worst bound for `m % n` is $\frac{m}{2}$, so the worst case recursive call becomes `gcd(m, m/2)`. Since $m \mod n \neq 0$, our next recursive call is `gcd(m % n, n % (m % n))`. By applying part a, we know this call is bounded above by `gcd(m / 2, n % (m / 2))`. `n % (m / 2)` is bounded above trivially by `m / 2`, so the worst case recursive call becomes `gcd(m / 2, m / 2)`. The worst case recursive calls then become `gcd(m, n)`, `gcd(n, m / 2)`, `gcd(m / 2, m / 2)`. Since the base case checks whether the second argument is 0, we notice that the second argument halves every two calls i.e. after $2k$ steps, the worst case of the second argument is $\frac{m}{2^k}$. When $\frac{m}{2^k} < 1$, the base case will trigger. Solving the inequality, we get that $k > \log_2 m$. This means we will need at least $2k = 2\log_2 m$ steps to trigger the base case, and since the program stops recursing once the base case is reached, the Euclidean Algorithm will make at most $2\log_2 m$ recursive calls in the worst case. □

3: Around and Around Again

Find the multiplicative inverse of $n-1 \mod n$ for $n \geq 2$

We define the multiplicative inverse as m where $m \in \mathbb{Z}$. Let $m = n-1$. We will show that m is the multiplicative inverse of $n-1 \mod n$.

For m to be the multiplicative inverse of $n-1 \mod n$, we have to show that $(m*(n-1 \mod n)) \mod n = 1$.

$$
\begin{aligned}
(m*(n-1 \mod n)) \mod n &= (m \mod n * n-1 \mod n) \mod n \\
&= m*n-1 \mod n && \text{[multiplicativity of mod]} \\
&= (n-1)(n-1) \mod n && \text{[definition of } m\text{]} \\
&= n^2-2n+1 \mod n \\
&= n^2 \mod n - 2n \mod n + 1 \mod n \\
&= 1 \mod n \\
&= 1
\end{aligned}
$$

Since we have shown that $(m*(n-1 \mod n)) = 1$, we have shown that $m = n-1$ is a multiplicative inverse of $n-1 \mod n$ for $n/geq2$.

□