0: 11 Modom

Claim: Every palindromic integer with an even number of digits is divisible by 11.

Let m be a palindromic integer with $2n$ (an even number) digits. We can write m as $x_1x_2...x_nx_n...x_2x_1$ where $x_1...x_n$ are individual digits. m can be rewritten using the base 10 representation of integers.

$$m = x_1 \cdot 10 + x_2 \cdot 10^1 + ... + x_n \cdot 10^{n-1} + x_n \cdot 10^n + ...x_2 \cdot 10^{2n} + x_1 \cdot 10^{2n+1}$$

Using the definition of modular congruence, we know that $10 \equiv_{11} -1$. Thus, if we take mod 11 from the above definition of m, we can replace the powers of 10 with -1.

$$\begin{gathered}(x_1 + x_2 \cdot 10^1 + ... + x_n \cdot 10^{n-1} + x_n \cdot 10^n + ...x_2 \cdot 10^{2n} + x_1 \cdot 10^{2n+1}) \mod 11 \\ = (x_1 + x_2 \cdot -1^1 + ... + x_n \cdot -1^{n-1} + x_n \cdot -1^n + ...x_2 \cdot -1^{2n} + x_1 \cdot -1^{2n+1}) \mod 11 \\ = (x_1 - x_2 + x_3... - x_n + x_n... - x_3 + x_2 - x_1) \mod 11 \text{ (Simplification)}\end{gathered}$$

Since m is palindromic, the terms cancel each other out and the above equation simplifies to 0 mod 11. Since $m \equiv_{11} 0$, we can say that $11|m$ by the definition of congruence. Thus, any palindromic integer with an even number of digits is divisible by 11.

1: Too Many Twos

(a) Claim: In a fixed-width two's complement representation with n bits, any integer can be negated by flipping all bits and adding 1.

Let x be some arbitrary integer with n bits. We can write $x = b_{n-1}n_{n-2}...b_1b_0$. We can let x' be the negation of x with its digits flipped. x' can be represented as $x' = (1-b_{n-1})(1-b_{n-2})...(1-b_1)(1-b_0)$.

$$\begin{aligned} V(x') &= -(1-b_{n-1}) \cdot 2^{n-1} + \sum_{i=0}^{n-2}(1-b_i)2^i \\ &= -2^{n-1} + b_{n-1} \cdot 2^{n-1} + \sum_{i=0}^{n-2}(2^i - b_i \cdot 2^i) \\ &= -2^{n-1} + b_{n-1} \cdot 2^{n-1} + \sum_{i=0}^{n-2} 2^i + \sum_{i=0}^{n-2}(b_i \cdot 2^i) \end{aligned}$$

By finite geometric series, the term $\sum_{i=0}^{n-2} 2^i$ can be simplified to $\frac{1-2^{n-1}}{-1} = 2^{n-1} - 1$. Substituting this back into the previous equation, we get

$$\begin{aligned} V(x') &= -2^{n-1} + b_{n-1} \cdot 2^{n-1} + 2^{n-1} - 1 + \sum_{i=0}^{n-2}(b_i \cdot 2^i) \\ &= -1 + b_{n-1} \cdot 2^{n-1} + \sum_{i=0}^{n-2}(b_i \cdot 2^i) \end{aligned}$$

By the definition of V, $V(x) = b_{n-1} \cdot 2^{n-1} + \sum_{i=0}^{n-2}(b_i \cdot 2^i)$. Thus, the final equation becomes

$$\begin{gathered} V(x') = -1 + V(x) \\ V(x') + 1 = V(x) \end{gathered}$$

Thus, we have proved that in a fixed-width two's complement representation with n bits, any integer can be negated by flipping all bits and adding 1.

(b) Claim: Over the given range, negation is bijective.

To prove that negation is bijective, we must prove that it is both injective and surjective.
Injective: $f : X \to Y$ is considered injective iff for all $x, y \in X, f(x) = f(y) \Rightarrow x = y$ (Definition of injection). Let x and y be two arbitrary integers in the range $-2^{n-1} < x, y < 2^{n-1}$ and $f(x) = -x$ be the negation function. If we let $f(x) = f(y)$, then by the definition of f, $-x = -y$. Multiplying both sides by -1, we are left with $x = y$. Therefore, we have proved that for all x, y in the range that if $f(x) = f(y)$, then $x = y$. Since x and y were chosen randomly, this is proven for all $x, y \in X$. Thus, f is injective by the definition of injection.

Surjective: $f : X \to Y$ is considered surjective iff for all $y \in Y$, there exists $x \in X$ such that $f(x) = y$ (Definition of surjection). Let y be an arbitrary integer in the range $-2^{n-1} < y < 2^{n-1}$ and let $x = -y$. Multiplying both sides by -1, we get $-x = y$. By the definition of f, this means that $f(x) = y$. Since y is in the range $-2^{n-1} < y < 2^{n-1}$, it follows that x is also in the range $-2^{n-1} < x < 2^{n-1}$. Thus, there exists $x \in X$ such that $f(x) = y$. Since y was chosen randomly, this is proven for all $y \in Y$. Thus, f is surjective by the definition of surjection.

Since we have proved that negation is both injective and surjective, we have proved that it is bijective. This is a property that we would like to retain in a fixed-width number system. This means that the negation of -2^{n-1} cannot be represented using only n bits since the negation is 2^{n-1}, outside of the range $(-2^{n-1}, 2^{n-1})$.

2: OMgcd

(a) Let m and n be arbitary positive integers such that $n \leq m$. Prove that $m \bmod n \leq \frac{m}{2}$. There are two cases for m and n.

Case 1: $n \leq \frac{m}{2}$. By the division theorem, we know that $m \bmod n < n$. If $n \leq \frac{m}{2}$, it follows that $m \bmod n \leq \frac{m}{2}$.

Case 2: $n > \frac{m}{2}$. By the division theorem, we can state that $m = nq + r$, for $q, r \in \mathbb{Z}$ where $0 \leq r < n$. If we know $n > \frac{m}{2}$, it follows that $\frac{m}{n} < 2$ by rearranging the equation. We also know that $n \leq m$, and therefore, $\frac{m}{n} \geq 1$. If $1 \leq \frac{m}{n} < 2$, we know that q must equal 1. Substituting 1 for q, we have

$$m = n(1) + r = n + r \text{ (Substituting for q)}$$
$$m - n = r \text{ (Rearranging the equation)}$$

Since we know that $r = m \bmod n$ by the division theorem, we know that $m \bmod n = m - n < m - \frac{m}{2} = \frac{m}{2}$. Therefore, we have proved that $m \bmod n < \frac{m}{2}$.

Since m and n must fall into either case, we have proved that $m \bmod n \leq \frac{m}{2}$.

(b) Claim: The Euclidean Algorithm will make at most $2\log_2 m$ recursive calls.

Let m and n be arbitary positive integers such that $n \leq m$. At every recursive call of gcd(m, n), the next call is gcd(n, m mod n). From part a, we know that $m \bmod n \leq \frac{m}{2}$. Thus, for every call of gcd(m, n), the next recursive call will contain a second argument that is at most $\frac{m}{2}$. For the second argument to reach 0, the function will continue to recurse at most $\log_2 m + \log_2 n$ times since either n or m decreases by half each step. Since we know that $n \leq m$, it follows that $\log_2 m + \log_2 n \leq \log_2 m + \log_2 m = 2\log_2 m$. Thus, we have proven that the Euclidean Algorithm will make at most $2\log_2 m$ recursive calls.

3: Around and Around Again

Let m be the multiplicative inverse of $n - 1$ mod n for $n \geq 2$. By the definition of multiplicative inverse,

$$m(n-1) \equiv_n 1$$
$$mn - m \equiv_n 1$$

4: Freshman's Dream