Multiple of 35

The USSR Olympiad Problem Book, by D. O. Shklarski, N . N. Chentzov, and I. M. Yaglom.

#28. (a) Prove that $35 \mid (3^{6n} - 2^{6n})$ for every positive integer n.

Proof. By direct calculation:

$$\begin{aligned} 3^6 &\equiv 4 \equiv -1 \pmod 5, & 2^6 &\equiv 4 \equiv -1 \pmod 5 \\ 3^{12} &\equiv 1 \pmod 5, & 2^{12} &\equiv 1 \pmod 5 \\ 3^{18} &\equiv -1 \pmod 5, & 2^{18} &\equiv -1 \pmod 5 \\ 3^{24} &\equiv 1 \pmod 5, & 2^{24} &\equiv 1 \pmod 5. \end{aligned}$$

and the rows continue to oscillate between -1 and 1:

$$\begin{aligned} 3^{6n} &= (3^6)^n \equiv (-1)^n \pmod 5 \\ 2^{6n} &= (2^6)^n \equiv (-1)^n \pmod 5 \\ \therefore 3^{6n} - 2^{6n} &\equiv (-1)^n - (-1)^n \equiv 0 \pmod 5. \end{aligned}$$

That is, $5 \mid (3^{6n} - 2^{6n})$. Also:

$$\begin{aligned} 3^6 &= 729 \equiv 1 \pmod 7 \\ \therefore 3^{6n} &= \left(3^6\right)^n \equiv 1^n \equiv 1 \pmod 7. \end{aligned}$$

Similarly:

$$\begin{aligned} 2^6 &= 64 \equiv 1 \pmod 7 \\ \therefore 2^{6n} &= \left(2^6\right)^n \equiv 1^n \equiv 1 \pmod 7. \end{aligned}$$

Therefore $3^{6n} - 2^{6n} \equiv 1 - 1 \equiv 0 \pmod 7$; that is, $7 \mid (3^{6n} - 2^{6n})$. Since both 5 and 7 divide $3^{6n} - 2^{6n}$, 35 does as well. **QED.**

The solution in the book takes a different tack. Consider the identity:

$$x^4 - y^4 = (x+y)\left(x^3 - x^2y + xy^2 - y^3\right).$$

There is a similar identity for $x^{2n} - y^{2n}$ for $n = 1, 2, 3, \ldots$, so $(x+y) \mid (x^{2n} - y^{2n})$ as polynomials. Plugging in $x = 3^3 = 27,\ y = 2^3 = 8$:

$$\begin{aligned} \left(3^3 + 2^3\right) &\,\Big|\, \left(\left(3^3\right)^{2n} - \left(2^3\right)^{2n}\right) \\ \therefore 35 &\,\Big|\, \left(3^{6n} - 2^{6n}\right). \quad \textbf{QED.} \end{aligned}$$

(b) $120 \mid (n^5 - 5n^3 + 4n)$ for every integer n.

Proof. Factor the polynomial:

$$\begin{aligned} n^5 - 5n^3 + 4n &= n(n^4 - 5n^2 + 4) \\ &= n\left(n^2 - 1\right)\left(n^2 - 4\right) \\ &= n(n-1)(n+1)(n-2)(n+2) \qquad (1) \end{aligned}$$

The expression in equation (1) is a product of five consecutive integers, so 3 divides at least one of them and 5 divides one of them. Also, 4 divides at least one of them and 2 divides *another* one, so 8 divides the product. It follows that $3 \cdot 5 \cdot 8 = 120$ divides the product. **QED.**

(c)* $56,786,730 \mid mn(m^{60} - n^{60})$ for all integers m, n.

Proof. First is to note that $56,786,730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$. Put $M(m,n,p) = mn(m^{p-1} - n^{p-1})$ for integers m and n and prime p. It suffices to prove that each of those primes divides $M(m,n,61)$ for all integers m and n. Fermat's Little Theorem states that for any prime p:

$$a^p \equiv a \pmod{p} \text{ for any integer } a.$$

Letting $p = 61$ and setting a to m and then n, this becomes:

$$m^{61} \equiv m \pmod{61} \text{ for any integer } m,$$
$$n^{61} \equiv n \pmod{61} \text{ for any integer } n.$$

Therefore:

$$\begin{aligned} M(m,n,61) &= mn(m^{60} - n^{60}) \\ &= m^{61} \cdot n - m \cdot n^{61} \\ &\equiv \left(m^{61} \cdot n - m \cdot n^{61}\right) \pmod{61} \\ &\equiv (m \cdot n - m \cdot n) \pmod{61} \\ &\equiv 0 \pmod{61}. \end{aligned}$$

That is, $61 \mid M(m,n,61)$. Similarly $31 \mid M(m,n,31)$. But $M(m,n,31) \mid M(m,n,61)$ since $m^{60} - n^{60} = (m^{30} - n^{30})(m^{30} + n^{30})$. Therefore $31 \mid M(m,n,61)$. Exactly the same argument works for each of the primes in the factorization of 56,786,730, since for each of then, $(p-1) \mid 60$ and this implies that $M(m,n,p) \mid M(m,n,61)$. To see this, consider the identities:

$$\begin{aligned} a^2 - b^2 &= (a-b)(a+b) \\ a^3 - b^3 &= (a-b)(a^2 + ab + b^2) \\ a^4 - b^4 &= (a-b)(a^3 + a^2b + ab^2 + b^3) \\ &\vdots \\ a^n - b^n &= (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}), \quad n > 1. \end{aligned} \tag{2}$$

Equation (2) is proven by multiplying out the right side and cancelling like terms. This shows that $(a-b) \mid (a^n - b^n)$, which can be generalized to $s \mid r \implies (a^s - b^s) \mid (a^r - b^r)$. To see how this works, consider the example $r = 20,\ s = 4$. Make the substitutions $A = a^4,\ B = b^4$. Applying (2) for A, B and exponent 5 and substituting:

$$\begin{aligned} A^5 - B^5 &= (A - B)\left(A^4 + A^3B + A^2B^2 + AB^3 + B^4\right) \\ (a^4)^5 - (b^4)^5 &= \left(a^4 - b^4\right)\left((a^4)^4 + (a^4)^3b^4 + (a^4)^2(b^4)^2 + a^4(b^4)^3 + (b^4)^4\right) \\ a^{20} - b^{20} &= \left(a^4 - b^4\right)\left(a^{16} + a^{12}b^4 + a^8b^8 + a^4b^{12} + b^{16}\right). \end{aligned}$$

It follows from this that $M(m,n,p) \mid M(m,n,61)$ and $p \mid M(m,n,61)$ for all the other key primes, just like for 61 and 31 and therefore the same is true of their product; namely, $56,786,730 \mid M(m,n,61)$, where $M(m,n,61) = mn(m^{60} - n^{60})$. **QED**.

– Mike Bertrand
Jan 16, 2024