Proof. Using the Euclidean algorithm, we can write d in the form $ua + vc$, where u and v are integers. It is easy to see that one of the two numbers u, v is positive and the other is negative or zero. Without loss of generality, we may suppose that $u > 0$, $v \leq 0$. Now raise both sides of the congruence $b^a \equiv 1 \ mod \ m$ to the u-th power, and raise both sides of the congruence $b^c \equiv 1 \ mod \ m$ to the $(-v)$-th power. Now divide the resulting two congruences, obtaining: $b^{au-c(-v)} \equiv 1 \ mod \ m$. But $au + cv = d$, so the proposition is proved.

Proposition I.4.3. *If p is a prime dividing $b^n - 1$, then either* (i) $p | b^d - 1$ *for some* **proper** *divisor d of n, or else* (ii) $p \equiv 1 \ mod \, n$. *If $p > 2$ and n is odd, then in case (ii) one has $p \equiv 1 \ mod \ 2n$.*

Proof. We have $b^n \equiv 1 \ mod \ p$ and also, by Fermat's Little Theorem, we have $b^{p-1} \equiv 1 \ mod \ p$. By the above proposition, this means that $b^d \equiv 1 \ mod \ p$, where $d = g.c.d.(n, \ p-1)$. First, if $d < n$, then this says that $p \,|\, b^d - 1$ for a proper divisor d of n, i.e., case (i) holds. On the other hand, if $d = n$, then, since $d|p-1$, we have $p \equiv 1 \ mod \ n$. Finally, if p and n are both odd and $n \,|\, p-1$ (i.e., we're in case (ii)), then obviously $2n| \, p-1$.

We now show how this proposition can be used to factor certain types of large integers.

Examples

1. Factor $2^{11} - 1 = 2047$. If $p \,|\, 2^{11} - 1$, by the theorem we must have $p \equiv 1 \ mod \ 22$. Thus, we test $p = 23, \ 67, \ 89, \ldots$ (actually, we need go no farther than $\sqrt{2047} = 45.\cdots$). We immediately obtain the prime factorization of 2047: $2047 = 23 \cdot 89$. In a very similar way, one can quickly show that $2^{13} - 1 = 8191$ is prime. A prime of the form $2^n - 1$ is called a "Mersenne prime."
2. Factor $3^{12} - 1 = 531440$. By the proposition above, we first try the factors of the much smaller numbers $3^1 - 1$, $3^2 - 1$, $3^3 - 1$, $3^4 - 1$, and the factors of $3^6 - 1 = (3^3 - 1)(3^3 + 1)$ which do not already occur in $3^3 - 1$. This gives us $2^4 \cdot 5 \cdot 7 \cdot 13$. Since $531440/(2^4 \cdot 5 \cdot 7 \cdot 13) = 73$, which is prime, we are done. Note that, as expected, any prime that did not occur in $3^d - 1$ for d a proper divisor of 12 — namely, 73 – must be $\equiv 1 \ mod \ 12$.
3. Factor $2^{35} - 1 = 34359738367$. First we consider the factors of $2^d - 1$ for $d = 1, \ 5, \ 7$. This gives the prime factors 31 and 127. Now $(2^{35} - 1)/(31 \cdot 127) = 8727391$. According to the proposition, any remaining prime factor must be $\equiv 1 \ mod \ 70$. So we check 71, 211, 281,..., looking for divisors of 8727391. At first, we might be afraid that we'll have to check all such primes less than $\sqrt{8727391} = 2954.\cdots$. However, we immediately find that $8727391 = 71 \cdot 122921$, and then it remains to check only up to $\sqrt{122921} = 350.\cdots$. We find that 122921 is prime. Thus, $2^{35} - 1 = 31 \cdot 71 \cdot 127 \cdot 122921$ is the prime factorization.

Remark. In Example 3, how can one do the arithmetic on a calculator