(c) Find a sequence n_j approaching ∞ for which $lim_{j\longrightarrow\infty}\frac{\varphi(n_j)}{n_j} = 1$ and a sequence n_j for which $lim_{j\longrightarrow\infty}\frac{\varphi(n_j)}{n_j} = 0$.

24. Let N be an extremely large secret integer used to unlock a missile system, i.e., knowing N would enable one to launch the missiles. Suppose you have a commanding general and n different lieutenant generals. In the event that the commanding general (who knows N) is incapacitated, you want the lieutenant generals each to have enough partial information about N so that any three of them (but never two of them) can agree to launch the missiles.
(a) Let $p_1, \ldots, p_n$ be n different primes, all of which are greater than $\sqrt[3]{N}$ but much smaller than $\sqrt{N}$. Using the p_i, describe the partial information about N that should be given to the lieutenant generals.
(b) Generalize this system to the situation where you want any set of k ($k \geq 2$) of the lieutenant generals, working together, to be able to launch the missiles (but a set of $k-1$ of them can never unlock the system). Such a set-up is called a *k-threshold system for sharing a secret.*

4 Some applications to factoring

Proposition I.4.1. *For any integer b and any positive integer n, $b^n - 1$ is divisible by $b-1$ with quotient $b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1$.*

Proof. We have a polynomial identity coming from the following fact: 1 is a root of $x^n - 1$, and so the linear term $x-1$ must divide $x^n - 1$. Namely, polynomial division gives $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1)$. (Alternately, we can derive this by multiplying x by $x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1$, then subtracting $x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1$, and finally obtaining $x^n - 1$ after all the canceling.) Now we get the proposition by replacing x by b.

A second proof is to use arithmetic in the base b. Written to the base b, the number $b^n - 1$ consists of n digits $b-1$ (for example, $10^6 - 1 = 999999$). On the other hand, $b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1$ consists of n digits all 1. Multiplying $111\cdots111$ by the 1-digit number $b-1$ gives $(b-1)(b-1)(b-1)\cdots(b-1)(b-1)(b-1)_b = b^n - 1$.

Corollary. *For any integer b and any positive integers m and n, we have $b^{mn} - 1 = (b^m - 1)(b^{m(n-1)} + b^{m(n-2)} + \cdots + b^{2m} + b^m + 1)$.*

Proof. Simply replace b by b^m in the last proposition.

As an example of the use of this corollary, we see that $2^{35} - 1$ is divisible by $2^5 - 1 = 31$ and by $2^7 - 1 = 127$. Namely, we set $b = 2$ and either $m = 5$, $n = 7$ or else $m = 7$, $n = 5$.

Proposition I.4.2. *Suppose that b is prime to m, and a and c are positive integers. If $b^a \equiv 1$ mod m and $b^c \equiv 1$ mod m, and if $d = g.c.d.(a, c)$, then $b^d \equiv 1$ mod m.*