many ways to go about this. For example, k can be written in binary as $a_0 + a_1 \cdot 2 + \cdots + a_{m-1}2^{m-1}$, then P can be successively doubled, with $2^j P$ added to the partial sum whenever the corresponding bit a_j is 1. Alternately, k could be factored first into a product of primes ℓ_j, and then one could successively compute $\ell_1(P)$, $\ell_2(\ell_1 P)$, and so on, where $\ell_1, \ell_2, \ldots$ are the primes in the factorization (listed, say, in non-decreasing order). Here each multiple $\ell_j P_j$, where $P_j = \ell_{j-1}\ell_{j-2}\cdots\ell_1 P$, is computed by writing ℓ_j in binary and using repeated doublings.

We shall suppose that some such technique has been chosen to compute multiples kP.

We shall consider the point P and all of its multiples modulo n. This means that we let $P \ mod \ n = (x \ mod \ n, y \ mod \ n)$, and, every time we compute some multiple kP, we really compute only the reduction of the coordinates modulo n. In order to be able to work modulo n, there is a nontrivial condition that must hold whenever we perform a doubling step or add two different points. Namely, all denominators must be prime to n.

Proposition VI.3.1. *Let E be an elliptic curve with equation $y^2 = x^3 + ax + b$, where $a, b \in \mathbf{Z}$ and $g.c.d.(4a^3 + 27b^2, n) = 1$. Let P_1 and P_2 be two points on E whose coordinates have denominators prime to n, where $P_1 \neq -P_2$. Then $P_1 + P_2 \in E$ has coordinates with denominators prime to n if and only if there is no prime $p|n$ with the following property: the points $P_1 \ mod \ p$ and $P_2 \ mod \ p$ on the elliptic curve $E \ mod \ p$ add up to the point at infinity $O \ mod \ p \in E \ mod \ p$. Here $E \ mod \ p$ denotes the elliptic curve over $\mathbf{F}_p$ obtained by reducing modulo p the coefficients of the equation $y^2 = x^3 + ax + b$.*

Proof. First suppose that $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and $P_1 + P_2 \in E$ all have coordinates with denominators prime to n. Let p be any prime divisor of n. We must show that $P_1 \ mod \ p + P_2 \ mod \ p \neq O \ mod \ p$. If $x_1 \not\equiv x_2 \ mod \ p$, then, according to the description of the addition law on $E \ mod \ p$, we immediately conclude that $P_1 \ mod \ p + P_2 \ mod \ p$ is not the point at infinity on $E \ mod \ p$. Now suppose that $x_1 \equiv x_2 \ mod \ p$. First, if $P_1 = P_2$, then the coordinates of $P_1 + P_2 = 2P_1$ are found by the formula (5) of §1, and $2P_1 \ mod \ p$ is found by the same formula with each term replaced by its residue modulo p. We must show that the denominator $2y_1$ is not divisible by p. If it were, then, because the denominator of the x-coefficient of $2P_1$ is not divisible by p, it would follow that the numerator $3x_1^2 + a$ would be divisible by p. But this would mean that x_1 is a root modulo p of both the cubic $x^3 + ax + b$ and its derivative, contradicting our assumption that there are no multiple roots modulo p. Now suppose that $P_1 \neq P_2$. Since $x_2 \equiv x_1 \ mod \ p$ and $x_2 \not\equiv x_1$, we can write $x_2 = x_1 + p^r x$ with $r \geq 1$ chosen so that neither the numerator nor denominator of x is divisible by p. Because we have assumed that $P_1 + P_2$ has denominator not divisible by p, we can use the formula (4) of §1 to conclude that y_2 is of the form $y_1 + p^r y$. On the other hand,