The following example is from Trappe & Washington (2006), with some details added.

We want to factor $n = 455839$. Let's choose the elliptic curve $y^2 = x^3 + 5x - 5$, with the point $P = (1, 1)$ on it, and let's try to compute $(10!)P$.

The slope of the tangent line at some point *A*=(*x*, *y*) is $s = (3x^2 + 5)/(2y) \pmod{n}$. Using *s* we can compute 2*A*. If the value of *s* is of the form *a/b* where *b* > 1 and gcd(*a*,*b*) = 1, we have to find the modular inverse of *b*. If it does not exist, gcd(*n*,*b*) is a non-trivial factor of *n*.

First we compute 2*P*. We have $s(P) = s(1,1) = 4$, so the coordinates of $2P = (x', y')$ are $x' = s^2 - 2x = 14$ and $y' = s(x - x') - y = 4(1 - 14) - 1 = -53$, all numbers understood $\pmod{n}$. Just to check that this 2*P* is indeed on the curve: $(-53)^2 = 2809 = 14^3 + 5 \cdot 14 - 5$.

Then we compute 3(2*P*). We have $s(2P) = s(14,\text{-}53) = -593/106 \pmod{n}$. Using the Euclidean algorithm: 455839 = 4300·106 + 39, then 106 = 2·39 + 28, then 39 = 28 + 11, then 28 = 2·11 + 6, then 11 = 6 + 5, then 6 = 5 + 1. Hence gcd(455839, 106) = 1, and working backwards (a version of the extended Euclidean algorithm): 1 = 6 – 5 = 2·6 – 11 = 2·28 – 5·11 = 7·28 – 5·39 = 7·106 – 19·39 = 81707·106 – 19·455839. Hence $106^{-1} = 81707 \pmod{455839}$, and –593/106 = –133317 (mod 455839). Given this *s*, we can compute the coordinates of 2(2*P*), just as we did above: $4P = (259851, 116255)$. Just to check that this is indeed a point on the curve: $y^2 = 54514 = x^3 + 5x - 5 \pmod{455839}$. After this, we can compute $3(2P) = 4P \boxplus 2P$.

We can similarly compute 4!*P*, and so on, but 8!*P* requires inverting 599 (mod 455839). The Euclidean algorithm gives that 455839 is divisible by 599, and we have found a factorization 455839 = 599·761.

The reason that this worked is that the curve (mod 599) has $640 = 2^7 \cdot 5$ points, while (mod 761) it has 777 = 3·7·37 points. Moreover, 640 and 777 are the smallest positive integers *k* such that $kP = \infty$ on the curve (mod 599) and $\pmod{761}$, respectively. Since 8! is a multiple of 640 but not a multiple of 777, we have $8!P = \infty$ on the curve (mod 599), but not on the curve (mod 761), hence the repeated addition broke down here, yielding the factorization.