$g.c.d.(j_2, n) = 1$. The number of possible j_1's is $\varphi(m)$, and the number of possible j_2's is $\varphi(n)$. So the number of pairs is $\varphi(m)\varphi(n)$. This proves the corollary.

Since every n can be written as a product of prime powers, each of which has no common factors with the others, and since we know the formula $\varphi(p^\alpha) = p^\alpha(1 - \frac{1}{p})$, we can use the corollary to conclude that for $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$:

$$\varphi(n) = p_1^{\alpha_1}\Big(1 - \frac{1}{p_1}\Big)p_2^{\alpha_2}\Big(1 - \frac{1}{p_2}\Big)\cdots p_r^{\alpha_r}\Big(1 - \frac{1}{p_r}\Big) = n\prod_{p|n}\Big(1 - \frac{1}{p}\Big).$$

As a consequence of the formula for $\varphi(n)$, we have the following fact, which we shall refer to later when discussing the RSA system of public key cryptography.

Proposition I.3.4. *Suppose that n is known to be the product of two distinct primes. Then knowledge of the two primes p, q is equivalent to knowledge of $\varphi(n)$. More precisely, one can compute $\varphi(n)$ from p, q in $O(\log n)$ bit operations, and one can compute p and q from n and $\varphi(n)$ in $O(\log^3 n)$ bit operations.*

Proof. The proposition is trivial if n is even, because in that case we immediately know $p = 2$, $q = n/2$, and $\varphi(n) = n/2 - 1$; so we suppose that n is odd. By the multiplicativity of φ, for $n = pq$ we have $\varphi(n) = (p-1)(q-1) = n+1-(p+q)$. Thus, $\varphi(n)$ can be found from p and q using one addition and one subtraction. Conversely, suppose that we know n and $\varphi(n)$, but not p or q. We regard p, q as unknowns. We know their product n and also their sum, since $p + q = n + 1 - \varphi(n)$. Call the latter expression $2b$ (notice that it is even). But two numbers whose sum is $2b$ and whose product is n must be the roots of the quadratic equation $x^2 - 2bx + n = 0$. Thus, p and q equal $b \pm \sqrt{b^2 - n}$. The most time-consuming step is the evaluation of the square root, and by Exercise 16 of § I.1 this can be done in $O(\log^3 n)$ bit operations. This completes the proof.

We next discuss a generalization of Fermat's Little Theorem, due to Euler.

Proposition I.3.5. *If $g.c.d.(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \bmod m$.*

Proof. We first prove the proposition in the case when m is a prime power: $m = p^\alpha$. We use induction on α. The case $\alpha = 1$ is precisely Fermat's Little Theorem (Proposition I.3.2). Suppose that $\alpha \geq 2$, and the formula holds for the $(\alpha - 1)$-st power of p. Then $a^{p^{\alpha-1}-p^{\alpha-2}} = 1 + p^{\alpha-1}b$ for some integer b, by the induction assumption. Raising both sides of this equation to the p-th power and using the fact that the binomial coefficients in $(1+x)^p$ are each divisible by p (except in the 1 and x^p at the ends), we see that $a^{p^\alpha - p^{\alpha-1}}$ is equal to 1 plus a sum with each term divisible by p^α. That is, $a^{\varphi(p^\alpha)} - 1$ is divisible by p^α, as desired. This proves the proposition for prime powers.