Groups of order $pq$

If $|G| = pq$ for $p, q$ primes where $p > q$ then we can classify the possible isomorphism type of $G$. First, the number of Sylow $p$-subgroups of $G$ is a value $n_p$ with the property that $n_p \equiv 1 \pmod{p}$ and that $n_p | |G|$, which means $n_p | q$ and since $p > q$ implies that $n_p = 1$. As such there is a unique, hence normal subgroup $N \triangleleft G$ where $|N| = p$ and also $|G/N| = q$. Since $\gcd(|N|, |G/N|) = 1$ then by the Schur-Zassenhaus lemma, there also exists a subgroup $Q \leq G$ where $|Q| = |G/N| = q$. So if we let $N = \langle x \rangle$ and $Q = \langle y \rangle$ then $G = NQ$ where $G = \{x^i y^j \mid i \in \mathbb{Z}_p, j \in \mathbb{Z}_q\}$ as a set. The question is what is the group structure of $G$.

Since $N \triangleleft G$ then $yxy^{-1} = x^u$ where $u$ is a power such that $x^u$ is also a generator of $N$. As such $u \in U_p = \langle v \rangle^p = \{1, \ldots, p - 1\}$ which means that $yx = x^u y$ and that, in terms of group presentations

$$G = \langle x, y \mid x^p = 1, y^q = 1, yx = x^u y \rangle$$

where the relation $yx = x^u y$ tells us how to multiply $(x^i y^j)x^k y^l$. The question is how many possible distinct groups do we have, which comes down to determining the possibilities for $u$.

A basic fact to keep in mind is that $U_p = \langle v \rangle$, a cyclic group of order $\phi(p)$ under multiplication. We’ll see the importance of this in a bit. Since $yxy^{-1} = x^u$ then $y^qy^{-q} = x^u$ but since $|y| = q$ this means that $x = x^u$ which means that $u^q = 1$ in $U_p$. If $u = 1$ then this is automatic, and it also implies that $yxy^{-1} = x$ so that $yx = xy$ making $G$ abelian and isomorphic to $C_p \times C_q \cong C_{pq}$.

If $u \neq 1$ then $u^q = 1$ and $u^{p-1} = 1$ implies that $|u||(p-1)$ and $|u||q$ which means $|u| = q$ and therefore that $q|(p-1)$. It also means that $u \in \langle v^{\frac{p-1}{q}} \rangle$ since $|v| = p - 1$ implies $|v^{\frac{p-1}{q}}| = q$ and so $u = v^{a\frac{p-1}{q}}$ so if we let $u_a = v^{a\frac{p-1}{q}}$ for each $a \in 1, \ldots, p-1$ then $u_a^n = 1$ and thus $yxy = x^{u_a}$ is possible, and thus we can define

$$G_a = \langle x, y \mid x^p = 1, y^q = 1, yx = x^{u_a} y \rangle$$
where we observe that $u_a u_b = u_{a+b}$. The final fact to establish is that all the $G_a$ (for $a > 1$) are isomorphic to $G_1$. Specifically for $a \in 1, \ldots, p-1$ define $\psi : G_1 \to G_a$ by $\psi(y) = y$ and $\psi(x) = x^{u_{a-1}}$ since then $\psi(xy^{-1}) = \psi(x^{u_1}) = x^{u_1u_{a-1}} = x^{u_a}$ and $\psi(x)^{u_1} = x^{u_{a-1}u_1} = x^{u_a}$. Thus all $G_a$ are isomorphic and there are exactly two isomorphism classes of groups of order $pq$ overall, $C_p \times C_q$ and the metabelian group $G_1$. \hfill \Box