Theorem. *Let $k \in \mathbb{N}$, let l be sufficiently large (i.e. $l > l_0(k)$), and let R be a random set of l^{3k^2} words of length l in the letters x, y, x^{-1} and y^{-1}. Then*

$$\lim_{l\to\infty} \mathbb{P}(\langle x, y|R\rangle \textit{ has a quotient of the form } SO_k(\mathbb{Z}/p)) = 0$$

Proof. Examine $\mathrm{SO}_k(\mathbb{C})$, and let E_j be the event that there are two matrices A and B, not $(\pm 1, \pm 1)$, that satisfy the first j words in R. Since these (random) words can be thought of as (random) polynomial equations in $2k^2$ variables, E_j is a (random) variety in $\mathbb{C}^{2k^2}$. By Bezout's theorem, E_j has no more than l^{2k^2} irreducible components. Let (A, B) be a point, different from $(\pm 1, \pm 1)$ in E_j. Examine the event that $(A, B) \in E_{j+1}$, conditioned on E_j. Since we have added a new word which is independent of the existing words, we can use the following lemma:

Lemma. *Let G be any regular graph with more than 2 vertices, and let x be some vertex of G. Let $l > 1$. Then*

$$\mathbb{P}^x(R(l) = x) < \frac{1}{2}$$

(where $\mathbb{P}^x$ is the probability when starting from x)

Proof. This is more-or-less standard, and I don't feel like writing a proof now. □

The lemma gives that

$$\mathbb{P}((A, B) \in E_{j+1} \mid (A, B) \in E_j) < \frac{1}{2}$$

just by applying it to the graph G which is the Cayley graph of the group $\langle A, B\rangle$ with the generators A and B. Hence with probability $\geq \frac{1}{2}$, adding one relation breaks the irreducible component containing (A, B) into further irreducible components, which then must have smaller dimension.

Returning to Bezout's theorem, we see that after adding $2k^2 \log l$ words, with high probability one breaks all components. Therefore the maximal degree decreases by 1. Repeating this a further $2k^2$ times, the maximal degree of any component which is not $(\pm 1, \pm 1)$ is -1, so they are in fact empty. So we see that $4k^4 \log l$ words are enough to remove all solutions.

Now, the fact that there are no solutions in $\mathrm{SO}_k(\mathbb{C})$ shows that there are only finitely many p such that there is a solution for our system of equations. To strengthen the claim to any p, we use an effective version of the Nullstellensatz, say due to Berenstein & Yger (1991) — this was Nir Avni's contribution. Our polynomials have all coefficients in $\mathbb{Z}$ which are bounded by 2^l, their degrees are all l, and as explained above there are $m = 4k^4 \log l$ of them. Hence the effective Nullstellensatz says that one can find polynomials $q_1 \ldots, q_m \in \mathbb{Z}[x_1, \ldots, x_{2k^2}]$ such that $\sum p_i q_i \equiv b \in \mathbb{Z}$ and $b \leq e^{(Cl)^{2k^2}}$. Hence if $\mathrm{SO}_k(\mathbb{Z}/p)$ is a quotient of our random group $\langle x, y|R\rangle$ then p must divide b and in particular must be $\leq e^{(Cl)^{2k^2}}$. To remove these groups we use the generic argument that works for any finite group: just count all possible couples of elements of the finite group G, and for each show that it satisfies all equations with small probability, and sum all these probabilities. If we have $(Cl)^{2k^2}$ words, then this kills all finite groups smaller than $e^{(Cl)^{2k^2}}$.

There is some cheating here around the values $(\pm 1, \pm 1)$ — our system of polynomials equations does have these 4 solutions. The usual nullstellensatz therefore says that for $i \in \{1, \ldots, 2k^2\}$ the polynomial x_i or $x_i^2 - 1$ (depending on whether i corresponds to an on- or off-diagonal matrix element), or some power of it, can be written as $\sum p_j q_j$. So the question remains if this also has an effective version — I think I saw something like that too, but I don't feel like looking for it now.

The same general plan works in $\mathrm{SL}_k(\mathbb{Z}/p)$, the only difference is that the degrees of the polynomials are no longer l, because of the horrible determinants of minors that appear in the inverses, but they are still bounded by lk so a similar argument goes through. □