1150-68-528 **Eric Bach** and **Robert A Threlfall*** (rthrelfall@secure-systems.org), 955 Broadway Drive, Sun Prairie, WI 53590. *Derandomizing quadratic nonresidue construction: Progress and limitations.* Preliminary report.

For odd primes p, finding a quadratic nonresidue (QNR) using randomness is easy, as half the elements of $\mathbb{F}_p^*$ are QNR's. By 1796 Gauss knew, via quadratic reciprocity, that for $p \not\equiv 1 \pmod{24}$ the set $\{-1, 2, 3\}$ contains a QNR.

In 1985 Schoof, by elliptic curve point counting, showed for fixed $a \in \mathbb{Z}$, $\sqrt{a} \pmod{p}$ is computable in deterministic polynomial time (P); thus, for $p \equiv 9 \pmod{16}$ the 8th roots of unity: $\pm(1 \pm \mathrm{i})/\sqrt{2}$ are QNR's computable in P. In 2009 Sze, using Schoof's result, proved for $p \equiv 4 \pmod{5}$ that $(-5 - \sqrt{5})/2$ is a QNR computable in P.

Using other reciprocity laws, which predict the splitting of polynomials, we give formulas for QNR's computable in P, for primes represented by select binary quadratic forms. For example, for $p = x^2 + 16 \cdot 11y^2, y$ odd, $2 + \sqrt{22}$ is a QNR.

Also, we lessen the oracle complexity of QNR construction. The number of square roots mod p needed is reduced from $\lfloor \log_2(p-1) \rfloor$ to $\frac{1}{2}\lfloor \log_2(p-1) \rfloor - 2$.

Finally, we prove that direct application of a fixed number of reciprocity laws is never sufficient to universally construct a QNR computable in P. Infinitely many primes will always slip through. (Received July 15, 2019)