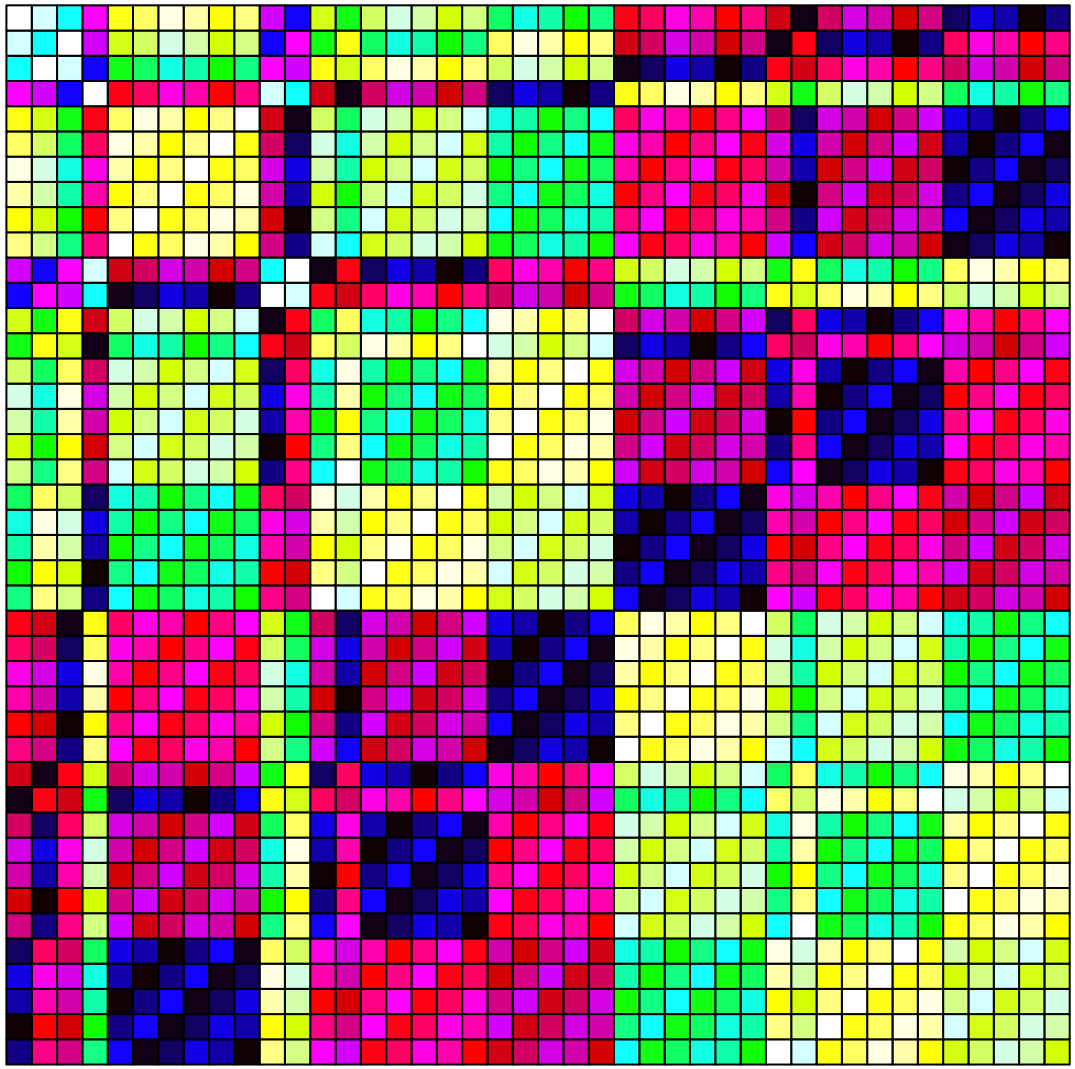
THEOREM OF THE DAY

A Theorem of Anderson, Cameron and Preece on Groups of Units *Let n be a prime of the form $6m+1$, $m>1$, and let α and β be the roots of x^2+3x+3 over $\mathbb{Z}_n$ (which exist by quadratic reciprocity). Then the group $\mathbb{U}_n$ of units of $\mathbb{Z}_n$ can be written as a direct product in the form $\mathbb{U}_n = \langle x\rangle_a \times \langle x+k\rangle_b \times \langle x+2k\rangle_c$, for some $x,k \in \mathbb{Z}_n$ and $\{a,b,c\} = \{2,3,m\}$, if and only if $m \equiv 1$ or $5 \pmod 6$ and one of the following occurs:*

1. *$ord(\alpha) = m$; then $x = -\alpha - 2$ and $k = \alpha + 1$.*
2. *$ord(\alpha/2) = m$; then $x = \alpha + 1$ and $k = -\alpha/2 - 1$.*
3. *$ord(\alpha) = n-1$ and $ord(\beta) = (n-1)/2$; then $x = 2\alpha + 3$ and $k = -\alpha - 2$.*



An element x of $\mathbb{Z}_n$ is a unit if $\gcd(x,n) = 1$. The units form a group $\mathbb{U}_n$ under multiplication mod n because each unit x has an order, $\text{ord}(x)$, such that $x^{\text{ord}(x)} = 1$ (so $x^{-1} = x^{\text{ord}(x)-1}$). The powers of a unit x form a cyclic subgroup of $\mathbb{U}_n$, which we can denote by $\langle x\rangle_{\text{ord}(x)}$. A collection of such subgroups whose orders multiply to give $|\mathbb{U}_n|$ and whose pairwise intersection is $\{1\}$ defines the whole group $\mathbb{U}_n$ via direct product. To illustrate for n prime, when every nonzero element of $\mathbb{Z}_n$ is a unit, suppose $n = 43$. Then $\text{ord}(6) = 3$ (since $6^3 = 216 \equiv 1 \pmod{43}$), $\text{ord}(42) = 2$ and $\text{ord}(35) = 7$. The direct product $\langle 6\rangle_3 \times \langle 42\rangle_2 \times \langle 35\rangle_7$ consists of the Cartesian product $\{1,6,36\} \times \{1,42\} \times \{1,35,21,4,11,41,16\}$, which may be enumerated as $(1,1,1), (6,1,1), (6^2,1,1), (1,42,1), (1,1,35), (1,1,35^2), (1,1,35^3), \ldots, (6^2,42,35^6)$, with elementwise multiplication, e.g. $(6,42,41)\cdot(36,42,11) = (1,1,21)$. This is indeed isomorphic to $\mathbb{U}_{43}$, the correspondence with the elements of $\mathbb{Z}_{43}$ specified by multiplication of triple entries, e.g. $(6,42,41) \to 6\times 42\times 41 = 12 \pmod{43}$. The multiplication table is depicted on the right with the elements represented by colours. You can discern the subgroups $\langle 6\rangle_3$, $\langle 42\rangle_2$ and $\langle 35\rangle_7$ in the top left corner.

Where does $\langle 35\rangle_7$ come from? The roots of x^2+3x+3 are $\left(-3 \pm \sqrt{-3}\right)\times 2^{-1}$. Now $2^{-1} = 22 \pmod{43}$ (because $2\times 22 = 44 \equiv 1 \pmod{43}$) and $\sqrt{-3} \equiv 13 \pmod{43}$ (because $13^2 = 169 \equiv 40 \equiv -3 \pmod{43}$; quadratic reciprocity tells us that -3 is a square modulo any prime congruent to 1 mod 6). So we can take $\alpha = (-3-13)\times 22 = -352 \equiv 35 \pmod{43}$. Since $\text{ord}(35) = 7$, part (1) of the theorem applies, with $x = -35-2 \equiv 6 \pmod{43}$ and $k = 36$.

And where does the quadratic x^2+3x+3 come from? We observe merely that if it has root α in $\mathbb{Z}_n$ then $(\alpha+1)^3 = \alpha(\alpha^2+3\alpha+3)+1 = 1$, and so $\text{ord}(\alpha+1) = 3$ in $\mathbb{Z}_n$.

Donald Arthur Preece collaborated with Ian Anderson (2011) and Peter Cameron (2013) in the subtle and intricate task of constructing $\mathbb{U}_n$ for various n in terms of units in arithmetic progression, of interest in experimental design theory as well as in number theory and combinatorics.

Web link: arxiv.org/abs/1111.3507 (section 2) builds on www.emis.de/journals/INTEGERS/papers/m52/m52.Abstract.html (e.g. Theorem 7).
Further reading: *Design of Comparative Experiments* by R.A. Bailey, Cambridge University Press, 2008.