Math Club Notes: 2007 April 4

1 Partial results on the cubes mod p

One of our outstanding problems considers the cubes mod p. With $p = 13$, we have

k	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
$k^3 \bmod 13$	5	5	1	-1	5	-1	0	1	-5	1	-1	-5	-5

With $p = 17$, we have

k	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8
$k^3 \bmod 17$	-2	-3	5	-6	4	7	-8	-1	0	1	8	-7	-4	6	-5	3	2

For $p = 13$, only some residues are cubes, and each nonzero cube has exactly three distinct cube roots. For $p = 17$, every residue is a cube, and has exactly one cube root. The questions are, well, the obvious ones; in short: how does this all work?

Today we saw some partial results about these phenomena.

Lemma 1 Every nonzero cube has the same number of cube roots.

Proof Let a^3 and b^3 be nonzero cubes. Let $A = \{z\colon z^3 = a^3\}$ be the set of cube roots of a^3, and let $B = \{z\colon z^3 = b^3\}$ be the set of cube roots of b^3. Define

$$\begin{aligned} \phi\colon A &\to B\,, \\ z &\mapsto za^{-1}b\,. \end{aligned}$$

ϕ is well-defined: first, a^{-1} is defined because $a \neq 0$ by hypothesis; second, if $z \in A$ then $z^3 = a^3$, so

$$(\phi(a))^3 = (za^{-1}b)^3 = z^3a^{-3}b^3 = a^3a^{-3}b^3 = b^3\,,$$

whence $\phi(a) \in B$. (Note that we use the commutativity of multiplication here.)

ϕ is bijective: its inverse is given by $\phi^{-1}(z) = zb^{-1}a$ (which is well-defined for similar reasons).

Thus A and B have the same number of elements, as claimed. □

Thus we can concentrate on the question of how many cube roots there are of, say, 1 (or any other nonzero residue known to be cube… 1 is the natural choice). We also immediately get the following:

Lemma 2 The number of cube roots of 1 in $\mathbb{Z}_p$ divides $p - 1$.

Proof There are $p - 1$ nonzero residues. Arrange them in sets according to their cubes (so that two nonzero residues are in the same set if and only if they have the same cube). Each of these sets is the set of cube roots of some nonzero cube. By the previous lemma, these sets are all the same size. Therefore that size divides $p - 1$. □

We can also prove lemma 2 by noting that the cube roots of 1 form a group under multiplication mod p, a subgroup of $U(p)$ (the set $\{1, \ldots, p-1\}$ under multiplication mod p), and applying Lagrange's theorem.

Lemma 3 1 has at most 3 cube roots.

Proof Since $\mathbb{Z}_p$ is a field, polynomials over $\mathbb{Z}_p$ have unique factorization and we can give the usual argument: every cube root of 1 corresponds to a linear factor of $t^3 - 1$, and there are at most 3 such factors. □

Lemma 4 1 has either 1 or 3 cube roots.

Proof If the only cube root of 1 is 1 itself, then we're done.

So suppose $z^3 = 1$ and $z \neq 1$. Since $(z^n)^3 = (z^3)^n = 1^n = 1$, all powers of z are cube roots of 1. Since $z^3 = 1$, the order of z divides 3, hence is either 1 or 3. Since $z \neq 1$, its order is not 1, so its order is 3. So there are at least 3 cube roots of 1, namely 1, z, and z^2. By the previous lemma, this means there are exactly 3 cube roots of 1. □

So, what we saw for $p = 13$ and $p = 17$ are the only two possibilities. Either all nonzero cubes have 1 cube root, as in $\mathbb{Z}_{17}$ (in which case every residue is a cube), or they all have 3 cube roots, as in $\mathbb{Z}_{13}$. By lemma 2, the latter is only possible if p is of the form $3k + 1$.

What we don't know yet is whether p being of the form $3k + 1$ is also sufficient to ensure that cubes have 3 cube roots in $\mathbb{Z}_p$. (It holds for smallish such p, though. Here "smallish" means "less than 25000 or so".)

Note, incidentally, that lemma 2 is the only thing so far that relies on the fact that we're talking about $\mathbb{Z}_p$ instead of some arbitrary field. $\mathbb{R}$ and $\mathbb{C}$, for example, also illustrate the two cases mentioned in lemma 4.