[06.1] Given a 3-by-3 matrix M with integer entries, find A, B integer 3-by-3 matrices with determinant ± 1 such that AMB is diagonal.

Let's give an *algorithmic*, rather than *existential*, argument this time, saving the existential argument for later.

First, note that given two integers x, y, not both 0, there are integers r, s such that $g = \gcd(x, y)$ is expressible as $g = rx + sy$. That is,

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} r & * \\ s & * \end{pmatrix} = \begin{pmatrix} g & * \end{pmatrix}$$

What we want, further, is to figure out what other two entries will make the second entry 0, *and* will make that 2-by-2 matrix invertible (in $GL_2(\mathbb{Z})$). It's not hard to guess:

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} r & -y/g \\ s & x/g \end{pmatrix} = \begin{pmatrix} g & 0 \end{pmatrix}$$

Thus, given $(x\ y\ z)$, there is an invertible 2-by-2 integer matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that

$$\begin{pmatrix} y & z \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \gcd(y, z) & 0 \end{pmatrix}$$

That is,

$$\begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} = \begin{pmatrix} x & \gcd(y, z) & 0 \end{pmatrix}$$

Repeat this procedure, now applied to x and $\gcd(y, z)$: there is an invertible 2-by-2 integer matrix $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ such that

$$\begin{pmatrix} x & \gcd(y, z) \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} \gcd(x, \gcd(y, z)) & 0 \end{pmatrix}$$

That is,

$$\begin{pmatrix} x & \gcd(y, z) & 0 \end{pmatrix} \begin{pmatrix} a' & b' & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \gcd(x, y, z) & 0 & 0 \end{pmatrix}$$

since *gcd*s can be computed iteratively. That is,

$$\begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \begin{pmatrix} a' & b' & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \gcd(x, y, z) & 0 & 0 \end{pmatrix}$$

Given a 3-by-3 matrix M, *right*-multiply by an element A_1 of $GL_3(\mathbb{Z})$ to put M into the form

$$MA_1 = \begin{pmatrix} g_1 & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}$$

where (necessarily!) g_1 is the *gcd* of the top row. Then *left*-multiply by an element $B_2 \in GL_3(\mathbb{Z})$ to put MA into the form

$$B_2 \cdot MA_1 = \begin{pmatrix} g_2 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$$

where (necessarily!) g_2 is the *gcd* of the left column entries of MA_1. Then right multiply by $A_3 \in GL_3(\mathbb{Z})$ such that

$$B_2MA_1 \cdot A_3 = \begin{pmatrix} g_3 & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}$$

where g_3 is the *gcd* of the top row of B_2MA_1. Continue. Since these *gcd*s divide each other successively

$$\ldots |g_3|g_2|g_1 \neq 0$$

and since any such chain must be finite, after finitely-many iterations of this the upper-left entry ceases to change. That is, for some $A, B \in GL_3(\mathbb{Z})$ we have

$$BMA = \begin{pmatrix} g & * & * \\ 0 & x & y \\ 0 & * & * \end{pmatrix}$$

and also g divides the top row. That is,

$$u = \begin{pmatrix} 1 & -x/g & -y/g \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in GL_3(\mathbb{Z})$$

Then

$$BMA \cdot u = \begin{pmatrix} g & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$$

Continue in the same fashion, operating on the lower right 2-by-2 block, to obtain a form

$$\begin{pmatrix} g & 0 & 0 \\ 0 & g_2 & 0 \\ 0 & 0 & g_3 \end{pmatrix}$$

Note that since the r, s such that $\gcd(x, y) = rx + sy$ can be found via Euclid, this whole procedure is *effective.* And it certainly applies to larger matrices, not necessarily square.

[06.2] Given a row vector $x = (x_1, \ldots, x_n)$ of integers whose *gcd* is 1, prove that there exists an n-by-n integer matrix M with determinant ± 1 such that $xM = (0, \ldots, 0, 1)$.

(*The iterative/algorithmic idea of the previous solution applies here, moving the gcd to the right end instead of the left.*)

[06.3] Given a row vector $x = (x_1, \ldots, x_n)$ of integers whose *gcd* is 1, prove that there exists an n-by-n integer matrix M with determinant ± 1 whose bottom row is x.

This is a corollary of the previous exercise. Given A such that

$$xA = \begin{pmatrix} 0 & \ldots & 0 & \gcd(x_1, \ldots, x_n) \end{pmatrix} = \begin{pmatrix} 0 & \ldots & 0 & 1 \end{pmatrix}$$

note that this is saying

$$\begin{pmatrix} * & \ldots & * \\ \vdots & & \vdots \\ * & \ldots & * \\ x_1 & \ldots & x_n \end{pmatrix} \cdot A = \begin{pmatrix} * & \ldots & * & * \\ \vdots & & \vdots & \vdots \\ * & \ldots & * & * \\ 0 & \ldots & 0 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} * & \dots & * \\ \vdots & & \vdots \\ * & \dots & * \\ x_1 & \dots & x_n \end{pmatrix} = \begin{pmatrix} * & \dots & * & * \\ \vdots & & \vdots & \vdots \\ * & \dots & * & * \\ 0 & \dots & 0 & 1 \end{pmatrix} \cdot A^{-1}$$

This says that x is the bottom row of the invertible A^{-1}, as desired.

[06.4] Show that $GL(2, \mathbb{F}_2)$ is isomorphic to the permutation group S_3 on three letters.

There are exactly 3 non-zero vectors in the space $\mathbb{F}_2^2$ of column vectors of size 2 with entries in $\mathbb{F}_2$. Left multiplication by elements of $GL_2(\mathbb{F}_2)$ permutes them, since the invertibility assures that no non-zero vector is mapped to zero. If $g \in GL_2(\mathbb{F}_2)$ is such that $gv = v$ for all non-zero vectors v, then $g = 1_2$. Thus, the map

$$\varphi : GL_2(\mathbb{F}_2) \to \text{permutations of the set } N \text{ of non-zero vectors in } \mathbb{F}_2^2$$

is *injective*. It is a group homomorphism because of the associativity of matrix multiplication:

$$\varphi(gh)(v) = (gh)v = g(hv) = \varphi(g)(\varphi(h)(v))$$

Last, we can confirm that the injective group homomorphism φ is also surjective by showing that the order of $GL_2(\mathbb{F}_2)$ is the order of S_3, namely, 6, as follows. An element of $GL_2(\mathbb{F}_2)$ can send any basis for $\mathbb{F}_2^2$ to any other basis, and, conversely, is completely determined by telling what it does to a basis. Thus, for example, taking the first basis to be the standard basis $\{e_1, e_2\}$ (where e_i has a 1 at the i^{th} position and 0s elsewhere), an element g can map e_1 to any non-zero vector, for which there are $2^2 - 1$ choices, counting *all* less 1 for the zero-vector. The image of e_2 under g must be linearly independent of e_1 for g to be invertible, and conversely, so there are $2^2 - 2$ choices for ge_2 (*all* less 1 for 0 and less 1 for ge_1). Thus,

$$|GL_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = 6$$

Thus, the map of $GL_2(\mathbb{F}_2)$ to permutations of non-zero vectors gives an isomorphism to S_3.

[06.5] Determine all conjugacy classes in $GL(2, \mathbb{F}_3)$.

First, $GL_2(\mathbb{F}_3)$ is simply the group of *invertible* k-linear endomorphisms of the $\mathbb{F}_3$-vectorspace $\mathbb{F}_3^2$. As observed earlier, conjugacy classes of endomorphisms are in bijection with $\mathbb{F}_3[x]$-module structures on $\mathbb{F}_3^2$, which we know are given by *elementary divisors*, from the Structure Theorem. That is, all the possible structures are parametrized by monic polynomials $d_1 | \dots | d_t$ where the sum of the degrees is the dimension of the vector space $\mathbb{F}_3^2$, namely 2. Thus, we have a list of irredundant representatives

$$\begin{cases} \mathbb{F}_3[x]/\langle Q\rangle & Q \text{ monic quadratic in } \mathbb{F}_3[x] \\ \\ \mathbb{F}_3[x]/\langle x-\lambda\rangle \oplus \mathbb{F}_3[x]/\langle x-\lambda\rangle & \lambda \in \mathbb{F}_3^\times \end{cases}$$

We *can* write the first case in a so-called rational canonical form, that is, choosing basis $1, x \bmod Q$, so we have two families

$$\begin{cases} (1) & \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} & b \in \mathbb{F}_3, \ a \in \mathbb{F}_3^\times \\ \\ (2) & \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} & \lambda \mathbb{F}_3^\times \end{cases}$$

But the first family can be usefully broken into 3 sub-cases, namely, depending upon the reducibility of the quadratic, and whether or not there are repeated roots: there are 3 cases

$$\begin{array}{rcl} Q(x) & = & \text{irreducible} \\ Q(x) & = & (x-\lambda)(x-\mu) \quad (\text{with } \lambda \neq \mu) \\ Q(x) & = & (x-\lambda)^2 \end{array}$$

And note that if $\lambda \neq \mu$ then (for a field k)

$$k[x]/\langle (x-\lambda)(x-\mu)\rangle \approx k[x]/\langle x-\lambda\rangle \oplus k[x]/\langle x-\mu\rangle$$

Thus, we have

$$\begin{cases} (1a) & \begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix} & x^2+ax+b \text{ irreducible in } \mathbb{F}_3[x] & \\ (1b) & \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} & \lambda \neq \mu \ \text{ both nonzero} & (\text{modulo interchange of } \lambda, \mu) \\ (1b) & \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} & \lambda \in \mathbb{F}_3^2 & \\ (2) & \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} & \lambda \in \mathbb{F}_3^\times & \end{cases}$$

One might, further, list the irreducible quadratics in $\mathbb{F}_3[x]$. By counting, we know there are $(3^2-3)/2 = 3$ irreducible quadratics, and, thus, the guesses x^2-2, x^2+x+1, and x^2-x+1 (the latter two being cyclotomic, the first using the fact that 2 is not a square mod 3) are all of them.

[06.6] Determine all conjugacy classes in $GL(3,\mathbb{F}_2)$.

Again, $GL_3(\mathbb{F}_2)$ is the group of *invertible* k-linear endomorphisms of the $\mathbb{F}_2$-vectorspace $\mathbb{F}_2^3$, and conjugacy classes of endomorphisms are in bijection with $\mathbb{F}_2[x]$-module structures on $\mathbb{F}_2^3$, which are given by *elementary divisors*. So all possibilities are parametrized by monic polynomials $d_1|\ldots|d_t$ where the sum of the degrees is the dimension of the vector space $\mathbb{F}_2^3$, namely 3. Thus, we have a list of irredundant representatives

$$\begin{cases} (1) & \mathbb{F}_2[x]/\langle Q\rangle & Q \text{ monic cubic in } \mathbb{F}_2[x] \\ (2) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle & \\ (3) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle & \end{cases}$$

since the only non-zero element of $\mathbb{F}_2$ is $\lambda = 1$. We *can* write the first case in a so-called rational canonical form, that is, choosing basis $1, x, x^2$ mod Q, there are three families

$$\begin{cases} (1) & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -b \\ 0 & 1 & -a \end{pmatrix} & x^3+ax^2+bx+1 \text{ in } \mathbb{F}_2[x] \\ (2) & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} & \\ (3) & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \end{cases}$$

It is useful to look in detail at the possible factorizations in case 1, breaking up the single summand into more summands according to relatively prime factors, giving cases

$$\begin{cases} (1a) & \mathbb{F}_2[x]/\langle x^3+x+1\rangle \\ (1a') & \mathbb{F}_2[x]/\langle x^3+x^2+1\rangle \\ (1b) & \mathbb{F}_2[x]/\langle (x-1)(x^2+x+1)\rangle \\ (1c) & \mathbb{F}_2[x]/\langle (x-1)^3\rangle \end{cases}$$

since there are just two irreducible cubics x^3+x+1 and x^3+x^2+1, and a unique irreducible quadratic, x^2+x+1. (The counting above tells the number, so, after any sort of guessing provides us with the right number of check-able irreducibles, we can stop.) Thus, the 6 conjugacy classes have irredundant matrix representatives

$$
\begin{array}{cccccccc}
(1a) & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & (1a') & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} & (1b) & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} & (1c) & \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \\
(2) & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} & (3) & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & & & &
\end{array}
$$

[06.7] Determine all conjugacy classes in $GL(4, \mathbb{F}_2)$.

Again, $GL_4(\mathbb{F}_2)$ is *invertible* k-linear endomorphisms of $\mathbb{F}_2^4$, and conjugacy classes are in bijection with $\mathbb{F}_2[x]$-module structures on $\mathbb{F}_2^4$, given by *elementary divisors*. So all possibilities are parametrized by monic polynomials $d_1|\ldots|d_t$ where the sum of the degrees is the dimension of the vector space $\mathbb{F}_2^4$, namely 4. Thus, we have a list of irredundant representatives

$$
\left\{
\begin{array}{cc}
\mathbb{F}_2[x]/\langle Q\rangle & Q \text{ monic quartic} \\
\mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)Q(x)\rangle & Q \text{ monic quadratic} \\
\mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle & \\
\mathbb{F}_2[x]/\langle Q\rangle \oplus \mathbb{F}_2[x]/\langle Q\rangle & Q \text{ monic quadratic} \\
\mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle &
\end{array}
\right.
$$

since the only non-zero element of $\mathbb{F}_2$ is $\lambda = 1$. We could write all cases using rational canonical form, but will not, deferring matrix forms till we've further decomposed the modules. Consider possible factorizations into irreducibles, giving cases

$$\begin{cases}
(1a) & \mathbb{F}_2[x]/\langle x^4+x+1\rangle \\
(1a') & \mathbb{F}_2[x]/\langle x^4+x^3+1\rangle \\
(1a'') & \mathbb{F}_2[x]/\langle x^4+x^3+x^2+x+1\rangle \\
(1b) & \mathbb{F}_2[x]/\langle (x-1)(x^3+x+1)\rangle \\
(1b') & \mathbb{F}_2[x]/\langle (x-1)(x^3+x^2+1)\rangle \\
(1c) & \mathbb{F}_2[x]/\langle (x-1)^2(x^2+x+1)\rangle \\
(1d) & \mathbb{F}_2[x]/\langle (x^2+x+1)^2\rangle \\
(1e) & \mathbb{F}_2[x]/\langle (x-1)^4\rangle \\
(2a) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)(x^2+x+1)\rangle \\
(2b) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^3\rangle \\
(3) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle \\
(4a) & \mathbb{F}_2[x]/\langle x^2+x+1\rangle \oplus \mathbb{F}_2[x]/\langle x^2+x+1\rangle \\
(4b) & \mathbb{F}_2[x]/\langle (x-1)^2\rangle \oplus \mathbb{F}_2[x]/\langle (x-1)^2\rangle \\
(5) & \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle \oplus \mathbb{F}_2[x]/\langle x-1\rangle
\end{cases}$$

since there are exactly three irreducible quartics (as indicated), two irreducible cubics, and a single irreducible quadratic. Matrices are, respectively, and unilluminatingly,

$$\begin{bmatrix} 0&0&0&1\\ 1&0&0&1\\ 0&1&0&0\\ 0&0&1&0 \end{bmatrix}
\begin{bmatrix} 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0\\ 0&0&1&1 \end{bmatrix}
\begin{bmatrix} 0&0&0&1\\ 1&0&0&1\\ 0&1&0&1\\ 0&0&1&1 \end{bmatrix}
\begin{bmatrix} 1&0&0&0\\ 0&0&0&1\\ 0&1&0&1\\ 0&0&1&0 \end{bmatrix}
\begin{bmatrix} 1&0&0&0\\ 0&0&0&1\\ 0&1&0&0\\ 0&0&1&1 \end{bmatrix}$$

$$\begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&1 \end{bmatrix}
\begin{bmatrix} 0&1&0&0\\ 1&1&0&0\\ 0&1&0&1\\ 0&0&1&1 \end{bmatrix}
\begin{bmatrix} 1&0&0&0\\ 1&1&0&0\\ 0&1&1&0\\ 0&0&1&1 \end{bmatrix}
\begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&1 \end{bmatrix}$$

$$\begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&1&1&0\\ 0&0&1&1 \end{bmatrix}
\begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&1&1 \end{bmatrix}
\begin{bmatrix} 0&1&0&0\\ 1&1&0&0\\ 0&0&0&1\\ 0&0&1&1 \end{bmatrix}
\begin{bmatrix} 1&0&0&0\\ 1&1&0&0\\ 0&0&1&0\\ 0&0&1&1 \end{bmatrix}
\begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix}$$

[06.8] Tell a p-Sylow subgroup in $GL(3, \mathbb{F}_p)$.

To compute the order of this group in the first place, observe that an automorphism (invertible endomorphism) can take any basis to any other. Thus, letting e_1, e_2, e_3 be the standard basis, for an automorphism g the image ge_1 can be any non-zero vector, of which there are $p^3 - 1$. The image ge_2 can be anything not in the span of ge_1, of which there are $p^3 = p$. The image ge_3 can be anything not in the span of ge_1 and ge_2, of which, because those first two were already linearly independent, there are $p^3 - p^2$. Thus, the order is

$$|GL_3(\mathbb{F}_p)| = (p^3-1)(p^3-p)(p^3-p^2)$$

The power of p that divides this is p^3. Upon reflection, a person might hit upon considering the subgroup of upper triangular *unipotent* (eigenvalues all 1) matrices

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

where the super-diagonal entries are all in $\mathbb{F}_p$. Thus, there would be p^3 choices for super-diagonal entries, the right number. By luck, we are done.

[06.9] Tell a 3-Sylow subgroup in $GL(3, \mathbb{F}_7)$.

As earlier, the order of the group is

$$(7^3-1)(7^3-7)(7^3-7^2) = 2^6 \cdot 3^4 \cdot 7^3 \cdot 19$$

Of course, since $\mathbb{F}_7^\times$ is cyclic, for example, it has a subgroup T of order 3. Thus, one might hit upon the subgroup

$$H = \{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} : a, b, c \in T\}$$

is a subgroup of order 3^3. Missing a factor of 3. But all the permutation matrices (with exactly one non-zero entry in each row, and in each column, and that non-zero entry is 1)

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

These normalize *all* diagonal matrices, and also the subgroup H of diagonal matrices with entries in T. The group of permutation matrices consisting of the identity and the two 3-cycles is order 3, and putting it together with H (as a semi-direct product whose structure is already described for us) gives the order 3^4 subgroup.

[06.10] Tell a 19-Sylow subgroup in $GL(3, \mathbb{F}_7)$.

Among the Stucture Theorem canonical forms for endomorphisms of $V = \mathbb{F}_7^3$, there are $\mathbb{F}_7[x]$-module structures

$$V \approx \mathbb{F}_7[x]/\langle \text{ irreducible cubic } C\rangle$$

which are *invertible* because of the irreducibility. Let α be the image of x in $\mathbb{F}_7[x]/\langle C\rangle$. Note that $\mathbb{F}_7[\alpha] = \mathbb{F}_7[x]/C$ also has a natural ring structure. Then the action of any $P(x)$ in $k[x]$ on V (via this isomorphism) is, of course,

$$P(x) \cdot Q(\alpha) = P(\alpha) \cdot Q(\alpha) = (P \cdot Q)(x) \bmod C(x)$$

for any $Q(x) \in \mathbb{F}_7[x]$. Since C is irreducible, there are no non-trivial zero divisors in the ring $\mathbb{F}_7[\alpha]$. Indeed, it's a field. Thus, $\mathbb{F}_7[\alpha]^\times$ *injects* to $\mathrm{End}_{\mathbb{F}_7} V$. The point of saying this is that, therefore, if we can find an element of $\mathbb{F}_7[\alpha]^\times$ of order 19 then we have an *endomorphism* of order 19, as well. And it is arguably simpler to hunt around in side $\mathbb{F}_{7^3} = \mathbb{F}_7[\alpha]$ than in groups of matrices.

To compute anything explicitly in $\mathbb{F}_{7^3}$ we need an irreducible cubic. Luckily, $7 = 1 \bmod 3$, so there are many non-cubes mod 7. In particular, there are only 2 non-zero cubes mod 7, ± 1. Thus, $x^3 - 2$ has no linear factor in $\mathbb{F}_7[x]$, so is irreducible. The *sparseness* (having not so many non-zero coefficients) of this polynomial will be convenient when computing, subsequently.

Now we must find an element of order 19 in $\mathbb{F}_7[x]/\langle x^3-2\rangle$. There seems to be no simple algorithm for choosing such a thing, but there is a reasonable probabilistic approach: since $\mathbb{F}_{7^3}^\times$ is cyclic of order $7^3-1=19\cdot 18$, if we pick an element g at random the probability is $(19-1)/19$ that its order will be *divisible* by 19. Then, whatever its order is, g^{18} will have order either 19 or 1. That is, if g^{18} is not 1, then it is the desired thing. (Generally, in a cyclic group of order $p\cdot m$ with prime p and p not dividing m, a random element g has probability $(p-1)/p$ of having order divisible by p, and in any case g^m will be either 1 or will have order p.)

Since elements of the ground field $\mathbb{F}_7^\times$ are all of order 6, these would be bad guesses for the random g. Also, the image of x has cube which is 2, which has order 6, so x itself has order 18, which is not what we want. What to guess next? Uh, maybe $g=x+1$? Can only try. Compute

$$(x+1)^{18} = (((x+1)^3)^2)^3 \bmod x^3-2$$

reducing modulo x^3-2 at intermediate stages to simplify things. So

$$g^3 = x^3+3x^2+3x+1 = 3x^2+3x+3 \bmod x^3-2 = 3\cdot(x^2+x+1)$$

A minor piece of luck, as far as computational simplicity goes. Then, in $\mathbb{F}_7[x]$,

$$g^6 = 3^2\cdot(x^2+x+1)^2 = 2\cdot(x^4+2x^3+3x^2+2x+1) = 2\cdot(2x+2\cdot 2+3x^2+2x+1)$$
$$= 2\cdot(3x^2+4x+5) = 6x^2+x+3 \bmod x^3-2$$

Finally,

$$g^{18} = (g^6)^3 = (6x^2+x+3)^3 \bmod x^3-2$$
$$= 6^3\cdot x^6 + (3\cdot 6^2\cdot 1)x^5 + (3\cdot 6^2\cdot 3 + 3\cdot 6\cdot 1^2)x^4 + (6\cdot 6\cdot 1\cdot 3 + 1^3)x^3 + (3\cdot 6\cdot 3^2 + 3\cdot 1^2\cdot 3)x^2 + (3\cdot 1\cdot 3^2)x + 3^3$$
$$= 6x^6+3x^5+6x^4+4x^3+3x^2+6x+6 = 6\cdot 4 + 3\cdot 2\cdot x^2 + 6\cdot 2x + 4\cdot 2 + 3x^2 + 6x + 6 = 2x^2+4x+3$$

Thus, if we've not made a computational error, the endomorphism given by multiplication by $2x^2+4x+3$ in $\mathbb{F}_7[x]/\langle x^3-2\rangle$ is of order 19.

To get a matrix, use (rational canonical form) basis $e_1=1$, $e_2=x$, $e_3=x^2$. Then the matrix of the endomorphism is

$$M = \begin{pmatrix} 3 & 4 & 1 \\ 4 & 3 & 4 \\ 2 & 4 & 3 \end{pmatrix}$$

Pretending to be brave, we check by computing the 19^{th} power of this matrix, modulo 7. Squaring repeatedly, we have (with determinants computed along the way as a sort of parity-check, which in reality did discover a computational error on each step, which was corrected before proceeding)

$$M^2 = \begin{pmatrix} 1 & 0 & 6 \\ 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \quad M^4 = \begin{pmatrix} 6 & 3 & 2 \\ 1 & 6 & 3 \\ 5 & 1 & 6 \end{pmatrix} \quad M^8 = \begin{pmatrix} 0 & 4 & 2 \\ 1 & 0 & 4 \\ 2 & 1 & 0 \end{pmatrix} \quad M^{16} = \begin{pmatrix} 6 & 5 & 5 \\ 6 & 6 & 5 \\ 6 & 6 & 6 \end{pmatrix}$$

Then

$$M^{18} = M^2\cdot M^{16} = \begin{pmatrix} 1 & 0 & 6 \\ 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}\cdot M^{16} = \begin{pmatrix} 6 & 5 & 5 \\ 6 & 6 & 5 \\ 6 & 6 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 4 & 0 & 1 \\ 4 & 4 & 0 \end{pmatrix}$$

$$M^{19} = M\cdot M^{18} = \begin{pmatrix} 3 & 4 & 1 \\ 4 & 3 & 4 \\ 2 & 4 & 3 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 & 1 \\ 4 & 0 & 1 \\ 4 & 4 & 0 \end{pmatrix} = \text{ the identity}$$

Thus, indeed, we have the order 19 element.

Note that, in reality, without some alternative means to verify that we really found an element of order 19, we could easily be suspicious that the numbers were wrong.