CHAPTER VI

Fermat's little theorem for matrices

6.1. Introduction.

We extend Fermat's little theorem to matrices, using the hyperintricate representation. The little theorem is simply extended in the real case and a proof is then given of its extension to intricate numbers (2 × 2 matrices). The intricate Euler totient formula is developed. The Fermat and Euler theorems for n-hyperintricate numbers are introduced, derived simply from the determinant. More explicit formulas are available here in the 'J-abelian' case.

6.2. The Chinese remainder theorem for eigenvalues.

The reader may wish to consult, by way of an introduction to the congruence arithmetic used in this chapter, the discussion in chapter III, sections 9 and 10.

Lemma. *If* $ka \equiv kb \pmod m$, *then*

$$a \equiv b \pmod{m/d}$$

where d *is the highest common factor of* k *and* m.

Proof. Suppose $k = k'd$, $m = m'd$, where k' is prime to m'. Then $(ka - kb)/m = k'd(a - b)/m'd = k'(a - b)/m'$, and then since k' is prime to m', $(a - b)$ must be a multiple of m', that is, $a \equiv b \pmod{m'}$, which is the same as $a \equiv b \pmod{m/d}$. □

Theorem. *Consider the set of simultaneous linear congruences involving unknown quantities*

$$a_1x_1 + a_2x_2 + ... + a_nx_n \equiv r_1 \pmod{m_1}$$
$$b_1x_1 + b_2x_2 + ... + b_nx_n \equiv r_2 \pmod{m_2}$$
$$...$$
$$g_1x_1 + g_2x_2 + ... + g_nx_n \equiv r_n \pmod{m_n}.$$

Let m *be the least common multiple of* $m_1, m_2, ... m_n$. Then by the lemma the given set of congruences may be replaced by the equivalent set

$$\frac{m}{m_1}a_1x_1 + \frac{m}{m_1}a_2x_2 + ... + \frac{m}{m_1}a_nx_n \equiv r_1 \pmod m$$
$$\frac{m}{m_2}b_1x_1 + \frac{m}{m_2}b_2x_2 + ... + \frac{m}{m_2}b_nx_n \equiv r_2 \pmod m$$
$$...$$
$$\frac{m}{m_n}g_1x_1 + \frac{m}{m_n}g_2x_2 + ... + \frac{m}{m_n}g_nx_n \equiv r_n \pmod m,$$

so that there is no loss of generality if the modulus is supposed to be the same for all congruences. *Then in the special case of an eigenvector equation*

$$A\mathbf{x} = \lambda\mathbf{x} \pmod m$$

the eigenvalues of this equation may be obtained (mod m). □

6.3. The intricate version of Fermat's little theorem.

Let r be an odd prime number.

We first consider the intricate number (2 × 2 matrix)

$$Я = a1 + bi + c\alpha + d\phi = a1 + J,$$

where the coefficients a, b, c and d are *integers*. Not all instances of integer 2×2 matrices adhere to this criterion, but for example all even 2×2 matrices satisfy it.

The intricate conjugate of $Я$ is

$$Я^* = a1 - bi - c\alpha - d\phi.$$

If $J^2 = (-b^2 + c^2 + d^2)$ *is non-zero* (mod r), *if it is a quadratic residue* (mod r), *then*

$$Я^r - Я \equiv 0 \pmod r$$

otherwise

$$Я^r - Я^* \equiv 0 \pmod r.$$

Note. Considerations below will show $(Я^r)^* = (Я^*)^r$.

Proof. The trivial case b = c = d = 0 is equivalent to $2^0 \times 2^0$ matrices, where the following proof is often given.

$$0^r - 0 \equiv 0 \pmod r,$$

so if

$$y^r - y \equiv 0 \pmod r,$$

then by the binomial theorem, since the denominators are not divisible by r,

$$(y + 1)^r - (y + 1) \equiv 0 \pmod r.$$

For intricate numbers, since a1 commutes with $J = (bi + c\alpha + d\phi)$, by the binomial theorem

$$Я^r = (a1)^r + [\text{terms multiplied by r}] + (bi + c\alpha + d\phi)^r.$$

Now

$$(bi + c\alpha + d\phi)^r = \{i(b1 + c\phi - d\alpha)\}^r.$$

The first two terms on the right expanded out become

$$-1(b1 - c\phi + d\alpha)(b1 + c\phi - d\alpha)1 = -(b^2 - c^2 - d^2)1.$$

Continuing the process gives

$$(bi + c\alpha + d\phi)^r = (-1)^{(r-1)/2}(b^2 - c^2 - d^2)^{(r-1)/2} i(b1 + c\phi - d\alpha)$$
$$= (-b^2 + c^2 + d^2)^{(r-1)/2}(bi + c\alpha + d\phi).$$

A standard result we will later prove for totients, is that $h^{(r-1)/2} \equiv 1 \pmod r$ when h is a quadratic residue (mod r) for instance a positive perfect square, and $\equiv -1 \pmod r$ when h is not a positive perfect square, or generally not a quadratic residue (mod r). Further, with equivalent statements on swapping positive and negative on the right of the next equivalence signs, if r = 4k – 1 with $h^{(r-1)/2} \equiv 1 \pmod r$ then $(-h)^{(r-1)/2} \equiv -1 \pmod r$, and if r = 4k + 1 with $h^{(r-1)/2} \equiv 1 \pmod r$ then $(-h)^{(r-1)/2} \equiv 1 \pmod r$. □

Whenever a prime r = 4k – 1 then because 1 is a square, if $-b^2 + c^2 + d^2 = 1 \pmod r$ then

$$(r + b^2 - c^2 - d^2)^{(r-1)/2} = (-1)^{(r-1)/2} \pmod r = -1 \pmod r,$$

which is not a quadratic residue. Likewise if $-b^2 + c^2 + d^2 = -1 \pmod r$ then $r + b^2 - c^2 - d^2 = 1 \pmod r$. But if r = 4k + 1 then when $-b^2 + c^2 + d^2 = 1 \pmod r$ then $r + b^2 - c^2 - d^2 = 1 \pmod r$, and when $-b^2 + c^2 + d^2 = -1 \pmod r$ then $r + b^2 - c^2 - d^2 = -1 \pmod r$.

Squares (mod r), that is, quadratic residues, are of the form $1.B = 1.A^2 \pmod r$, and thus it can be determined from the case $\neq 0 \pmod r$ whether $-1.A^2 \pmod r$ is or is not a quadratic residue.

Note that if a real number $A^2 = -b^2 + c^2 + d^2$, this implies

$$(A + c)(A - c) = (d + b)(d - b)$$

for linearly independent (A + c) and (A – c), and likewise respectively for (d + b) and (d – b).

Corollary. *For all integer* 2×2 *matrices with an intricate representation* $Я'$ *where* $J^2 = (-b^2 + c^2 + d^2)$ *is non-zero* (mod r), *if* J^2 *is a quadratic residue* (mod r), *then*

$$(2Я')^r - 2Я' \equiv 0 \text{ (mod r)} \qquad (1)$$

otherwise

$$(2Я')^r - 2Я'^* \equiv 0 \text{ (mod r). } \square \qquad (2)$$

Example. Let g be a Gaussian integer of the form a + ib, and g* be its complex conjugate. Then for prime p = 4k – 1

$$g^p - g^* \equiv 0 \text{ (mod p)},$$

since c = d = 0 and a and b are integers in the intricate representation, with $-b^2$ the negative of a perfect square, and therefore not a quadratic residue for this p.

6.4. Some synthetic generalisations of Fermat's little theorem.

We have for integer y and distinct odd primes p, q, r

$$(y^p - y)^q - (y^p - y) \equiv 0 \text{ (mod pq)}.$$

This can be written, ignoring binomial terms containing q, as

$$y^{pq} - y^q - y^p + y \equiv 0 \text{ (mod q)}.$$

Swapping p and q gives an identical expression on the left, so

$$y^{pq} - y^q - y^p + y \equiv 0 \text{ (mod pq)}. \qquad (1)$$

Suppose p is 2. Then still

$$y^p - y \equiv 0 \text{ (mod 2)}.$$

Thus

$$y^{pq} - y^q - y^p + y \equiv 0 \text{ (mod q)}$$

continues to hold. However

$$(y^p - y)^2 - (y^p - y) \equiv 0 \text{ (mod 2)},$$

which gives

$$y^{2q} - y^q + y^2 + y \equiv 0 \text{ (mod 2)},$$

with a different sign for y^2, which is not a problem because of the equivalence

$$y^2 \equiv -y^2 \text{ (mod 2)},$$

so that equation (1) continues to hold even for distinct p or q = 2.

Equation (1) can be generalised for distinct primes p, q, r to

$$y^{pqr} - [y^{qr} + y^{pr} + y^{pq}] + [y^p + y^q + y^r] - [y] \equiv 0 \text{ (mod pqr)}, \qquad (2)$$

with an obvious extension to n distinct odd primes, when the expressions in square brackets alternate in sign. $\square$

Corollary. *For all integer* 2×2 *matrices with an intricate representation* $Я'$ *where* $J^2 = (-b^2 + c^2 + d^2)$ *is non-zero* (mod p), (mod q) *and* (mod r), *if* J^2 *is a quadratic residue* (mod p), (mod q) *and* (mod r), *then*

$$(2Я')^{pqr} - [(2Я')^{qr} + (2Я')^{pr} + (2Я')^{pq}] + [(2Я')^p + (2Я')^q + (2Я')^r] - [2Я'] \equiv 0 \text{ (mod pqr). } \square$$

When we wish to determine a square (mod p^m), then

$$(y^p - y)^m \equiv 0 \text{ (mod } p^m),$$

where the left hand side is given by a binomial expansion. $\square$

If $y^p - y \equiv 0 \pmod p$, then

$$y^{n(p-1)+1} - y \equiv 0 \pmod p.$$

Proof. Since $y^{2p-1} - y^p = y^{p-1}(y^p - y)$ is divisible by p, the sum $(y^{2p-1} - y^p) + (y^p - y)$ is also, with the general result following by recursion. □

Example. Putting p = 3, we have for any odd natural number q, $y^q - y \equiv 0 \pmod 6$.

6.5. The intricate version of Euler's totient formula.

The following theorem can be deduced from pages 163-167 of [Bu89], although the material can be obtained from the earlier [1He33]. An insightful work is [1Ma1886].

Let ↑ be the exponential operator.

Let s > 1 *be a natural number and* y *an integer with* gcd(y, s) = 1 *or* lcm(y, s) = s. *Then if* s *has the prime factorisation*

$$s = (q_1\uparrow j_1)(q_2\uparrow j_2) \ldots (q_n\uparrow j_n)$$

for primes q_i, *and where the totient*

$$\varphi(s) = s(1 - 1/q_1)\,(1 - 1/q_2) \ldots (1 - 1/q_r)$$

then

$$y^{\varphi(s)+1} - y \equiv 0 \pmod s.$$

Proof. The above factorises as

$$y(y^{\varphi(s)} - 1) \equiv 0 \pmod s$$

so either $y \equiv 0 \pmod s$, which is the same way as putting lcm(y, s) = s, or otherwise gcd(y, s) = 1 and

$$y^{\varphi(s)} - 1 \equiv 0 \pmod s.$$ □

Corollary. *For* gcd(y, s) = 1, y^2 *belongs to the* $y^{\varphi(s)/2} \equiv 1 \pmod s$ *equivalence class. Otherwise for* gcd(y, s) = 1, *non quadratic residues satisfy* $y^{\varphi(s)/2} \equiv -1 \pmod s$.

Proof. φ(s) is even and

$$(y^2)^{\varphi(s)/2} - 1 \equiv (y^{\varphi(s)/2} - 1)(y^{\varphi(s)/2} + 1) \equiv 0 \pmod s.$$ □

Corollary. *If r is prime, so* φ(r) = r – 1, *when* J *is a quadratic residue* (mod r), $J^{(r-1)/2} \equiv 1$ (mod r), *whereas* $J^{(r-1)/2} \equiv -1$ (mod r) *when* J *is not a quadratic residue* (mod r). □

To prove the intricate version of Euler's totient formula, for elements with lcm(y, t) = t or gcd(y, t) = 1 with j > 0, q prime and q^j = t, we first argue that, *if* $J^2 = -b^2 + c^2 + d^2$ *is a quadratic residue* (mod t), *then*

$$Я\uparrow[\varphi(q^j) + 1] - Я \equiv 0 \pmod t \qquad (1)$$

otherwise

$$Я\uparrow[\varphi(q^j) + 1] - Я^* \equiv 0 \pmod t. \qquad (2)$$

Proof. If all elements are equivalent to 0 (mod t), then $Я \equiv 0 \pmod t$. So assume gcd(y, t) = 1 for at least one y = a, b, c or d, otherwise a, b, c or d ≡ 0 (mod t). Using the binomial theorem,

$$Я\uparrow[\varphi(q^j) + 1] = (a1)^{\varphi(s)+1} + (\varphi(s) + 1)[\text{intermediate binomial terms}] + (bi + c\alpha + d\phi)^{\varphi(s)+1}.$$

An argument similar to that for Fermat's little theorem gives

$$(bi + c\alpha + d\phi)^{\varphi(s)+1} = (-b^2 + c^2 + d^2)^{\varphi(s)/2}(bi + c\alpha + d\phi).$$

We have previously proved that if $(-b^2 + c^2 + d^2)$ is a quadratic residue $\neq 0 \pmod t$, then it belongs to the $(-b^2 + c^2 + d^2)^{\varphi(s)/2} \equiv 1 \pmod t$ equivalence class, otherwise if $\neq 0 \pmod t$ to the $-1 \pmod t$ equivalence class.

Notice that

$$\varphi(q^{j+1}) = q^{j+1} - q^j = q(q^j - q^{j-1}) = q\varphi(q^j),$$

so that for $j = 1$ the terms

$$(\varphi(t) + 1)[\text{intermediate binomial terms}]$$

are $\equiv 0 \pmod t$, and if assumed for j, they likewise satisfy this for $j + 1$.

Now *assume* $-b^2 + c^2 + d^2$ is a perfect square $\neq 0 \pmod{q_i\uparrow j_i}$ for each i, then

$$Я\uparrow\varphi(q_i\uparrow j_i) \equiv 1 \pmod{q_i\uparrow j_i}.$$

Noting that $\varphi(s)$ is divisible by $\varphi(q_i\uparrow j_i)$, raising both sides to the power $\varphi(s)/\varphi(q_i\uparrow j_i)$, we arrive at

$$Я^{\varphi(s)} \equiv 1 \pmod{q_i\uparrow j_i}.$$

Because the moduli are relatively prime, this leads to the relation

$$Я^{\varphi(s)} \equiv 1 \pmod{(q_1\uparrow j_1)(q_2\uparrow j_2) \ldots (q_n\uparrow j_n)}$$

or

$$Я^{\varphi(s)} \equiv 1 \pmod s.$$

If $Я \equiv 0 \pmod s$, then this possibility is incorporated in

$$Я^{\varphi(s)+1} \equiv Я \pmod s. \ \square$$

The following result is also proved in [Ad14]. *Let* $s > 1$ *be a natural number and* y *an integer. Then if* s *has the prime factorisation*

$$s = (q_1\uparrow j_1)(q_2\uparrow j_2) \ldots (q_n\uparrow j_n)$$

for primes q_i, *and where the totient*

$$\varphi(s) = s(1 - 1/q_1)(1 - 1/q_2) \ldots (1 - 1/q_r) \qquad (3)$$

then

$$\varphi(s)[y^{\varphi(s)+1} - y] \equiv 0 \pmod s. \qquad (4)$$

Proof. Consider first the case when y is coprime to s′. If $\alpha, \beta, \gamma, \ldots \lambda$ are the $\varphi(s')$ numbers which are prime to s′ and less than it, the products $y\alpha, y\beta, y\gamma, \ldots y\lambda$ are all coprime to s′; moreover we have seen no two of them are congruent (mod s′). Hence the products $y\alpha, y\beta, y\gamma, \ldots y\lambda$ are congruent to $\alpha, \beta, \gamma, \ldots \lambda$ in a different order, and therefore

$$y\alpha.y\beta.y\gamma \ldots y\lambda = \alpha.\beta.\gamma \ldots \lambda.$$

Dividing by $\alpha.\beta.\gamma \ldots \lambda$, which is coprime to s′, we obtain

$$y^{\varphi(s')} - 1 \equiv 0 \pmod{s'},$$

when y is coprime to s′.

In the case when y is not coprime to s″, derived from formula (3), with $s = s's''$ and only s′ coprime to y,

$$\varphi(s'')y \equiv 0 \pmod{s''}.$$

Then on using

$$\varphi(s) = \varphi(s')\varphi(s'') \text{ and } (\text{mod } s) = (\text{mod } s')(\text{mod } s''),$$

theorem (4) is obtained from

$$(y^{\varphi(s)} - 1) = (y^{\varphi(s')} - 1)(y^{\varphi(s) - \varphi(s')} + y^{\varphi(s) - 2\varphi(s')} + \ldots + 1). \ \square$$

6.6. Some hyperintricate versions of Fermat's little theorem.

Let $Я_n$ be an n-hyperintricate number. The inverse $Я_n^{-1}$ of a non-singular $2^n \times 2^n$ matrix $Я_n$ exists and is unique. Its denominator may be expressed as the determinant, det $|Я_n|$, of the matrix. If we wish to obtain a hyperintricate conjugate, $Я_n$*, so that even in the singular case det $|Я_n| = 0$

$$Я_n(Я_n^*) = \det |Я_n|,$$

then provided det $|Я_n| \neq 0$ the inverse is

$$Я_n^{-1} = (Я_n^*)/\det |Я_n|$$

with

$$Я_n Я_n^{-1} = 1.$$

Since from chapter II each individual element of $Я_n$ is expressible hyperintricately, in all cases the determinant can be computed. A formula for determining the hyperintricate inverse when it is expressed in a 'J-abelian' form similar to the one provided below is given in there in section 15. This states how the determinant, det $|Я_n|$, is derived from $Я_n$*. The general inverse has also been computed there in section 16.

Then since det $|Я_n|$ is a scalar, the standard Fermat and Euler formulas apply to it.

When an n-hyperintricate number is J-abelian, that is expressed in the form $\Sigma U_{V...W}$, where U, V ... W are intricate numbers, with all values of J identical for a particular layer, then powers of this entity are abelian, the n-hyperintricate conjugate is readily available, and considerations obtained next apply.

We will derive from chapter II the definition of a J-abelian n-hyperintricate number given by

$$Я_n = \Sigma(r = 1 \text{ to } \lceil 4^{n-1}/n \rceil) \otimes (k = 1 \text{ to } n)(a_{rk}1 + J_k L_{rk}),$$

where we are using the ceiling function, $\lceil 4^{n-1}/n \rceil$, and the composite layer operator $\otimes$, and convert it for the Fermat little theorem case. The intricate $J_k \in \{i, \alpha, \phi\}$ or J_k in integer $\mathcal{JAF}$ format, with J_k^2 an integer, are identical over r and independent over k, so that such numbers are abelian in their J_k components, and the standard binomial theorem holds. This means the arguments we have used for Fermat's little theorem as generalised from equations 6.4.(1) or (2) and the Euler totient formula generalised from 6.5.(1), (2) and (4), carry over to this case.

The intricate algebra expresses the 2×2 noncommutative matrix

$$x = a1 + bi + c\alpha + d\phi$$

as the matrix $x = a1 + JK$ where $J^2K^2 = -b^2 + c^2 + d^2$ and

$$J^2 = 0 \text{ or } \pm 1.$$

Then for $J^2 = -1$ the algebra works under the substitution $J \rightarrow i$, and the considerations for complex x carry over to these matrices.

If we take K^2 as an integer, then we can represent $\pm K$ in complex congruence arithmetic in the manner we devised in part 7 section 8 of [Ad14]. Further, the intricate conjugate of x is

$$x^* = a1 - bi - c\alpha - d\phi,$$

so that we can adopt equations in the intricate case with J replacing i, that is, in an intricate, or more generally J-abelian, congruence arithmetic.

Outside of this case, compression and taking eigenvalues, we cannot apply the reduction of an n-hyperintricate number to an intricate one.

We show in chapter XI that if a matrix X is symmetric, then a similarity transformation QXQ^{-1} for Q an orthogonal matrix (its inverse is its transpose) can bring it into diagonal form. Thus if p is prime

$$(QXQ^{-1})^p - (QXQ^{-1}) = Q(X^p - X)Q^{-1},$$

and provided the expression is in integers, or fractions can be expressed as integers (mod p), the diagonal entries satisfy Fermat's little theorem, so that

$$Q(X^p - X)Q^{-1} \equiv 0 \text{ (mod p). } \square$$

The totient theorem also holds for symmetric X. If s is a natural number, under the same type of constraints

$$\varphi(s)Q(X^{\varphi(s)+1} - X)Q^{-1} \equiv 0 \text{ (mod s). } \square$$

Any matrix may be represented uniquely as a sum of symmetric and antisymmetric parts. Since the square of an antisymmetric matrix $Y = y_{ij}$ satisfies

$$\sum_j y_{ij}y_{jk} = \sum_j (-y_{kj})(-y_{ji}),$$

its square is symmetric, so for Y^2 previous considerations apply. $\square$

6.7. Exercises.

(A) What is $\varphi(s)$ when s is prime?

(B) Assume for natural numbers n, $s \in \mathbb{N}$ that

$$\varphi(s)[y^{\varphi(s)+1} - y] \equiv 0 \text{ (mod s).} \quad (1)$$

Prove by induction that

$$\varphi(s)[y^{n\varphi(s)+1} - y] \equiv 0 \text{ (mod s).} \quad (2)$$

By induction we mean, prove a suitable starting example (say n = 1), assume (2) holds for n, and then prove for (n + 1).

Note that you cannot assume if (1) holds that either $\varphi(s)[y] = 0$ or $y^{\varphi(s)} - 1 \equiv 0$ (mod s), since say for (mod 6), $2 \times 3 = 0$, but $2 \neq 0$ (mod 6) and $3 \neq 0$ (mod 6). However, you could make such an assumption when s is prime.

(C) Show for a matrix W with a symmetric part U and an antisymmetric part V, giving

$$W = U + V,$$

that, say, a trailing layer of $p1 + q\alpha + r\phi$ can be applied to U which keeps its symmetric state, and a trailing layer of ti can be appended to V which makes the matrix also symmetric.

Hence using the results indicated above from chapter XI, show that there exists an orthogonal matrix Q with

$$\varphi(s)Q[(U_{p1 + q\alpha + r\phi} + V_{ti})^{n\varphi(s)+1} - (U_{p1 + q\alpha + r\phi} + V_{ti})]Q^{-1} \equiv 0 \text{ (mod s),}$$

provided Q and thus Q^{-1} are expressible (mod s).