MODULAR INTERPOLATION*

BY E. T. BELL

1. *Interpolation* mod m. Let m be a constant integer >1, and let $r_1, \cdots, r_s$ denote s distinct constant integers such that

$$0 \leqq r_i < m, \qquad (i = 1, \cdots, s, s \leqq m).$$

Let $k_1, \cdots, k_s$ represent any s constants. It is required to construct a function $f(x)$ which is defined when $0 < x \equiv r_i \bmod m$, $(i = 1, \cdots, s)$, and which is such that

$$(1) \qquad f(x) = k_i, \text{ when } x \equiv r_i \bmod m, \quad (i = 1, \cdots, s).$$

This $f(x)$ will be called a modular interpolation function for $(r_1, \cdots, r_s)$ mod m. Such functions occur frequently in the theory of numbers, and are usually constructed "by inspection." A straightforward method of constructing $f(x)$ in (1) is required, as "inspection" is impracticable in only moderately complicated instances.

There obviously is no loss of generality in assuming $x>0$ as above. For, if x were <0, a congruence $x \equiv r_i$ mod m could be replaced by $-x \equiv m - r_i$ mod m, which is the previous case.

The general formula for $f(x)$ in §3 in its unreduced form is as simple as Lagrange's for ordinary interpolation. The final reduced polynomial forms of modular interpolation formulas have (in general) simpler coefficients than their correspondents in ordinary interpolation. This is due to reduction by the proper moduli, which has no analog in the ordinary case.

2. *Notation*. The notations of §1 for m, s, r_i, k_i and the following are fixed throughout the paper. We write $\phi(m) = \tau$, the number of integers $\leqq m$ and prime to m; $\mu(1) = 1$, $\mu(m) = 0$ if m is divisible by a square >1, $\mu(m) = 1$ or -1 in the contrary case according as m is the product of an even or an odd number of primes (Möbius' function). The totitives (positive integers $\leqq m$ and prime to m) of m are denoted by $t_1 = 1$, $t_2, \cdots, t_\tau$. The polynomial in y of degree τ whose roots are the τ primitive mth roots of unity is denoted by $P(y)$,

* Presented to the Society, November 29, 1930.

$$(2)\qquad P(y) = \prod(y^d - 1)^{\mu(\delta)} = y^\tau + a_1 y^{\tau-1} + \cdots + a_\tau,$$

the product referring to all pairs (d, δ) of positive divisors of m such that $m = d\delta$. The coefficients $a_1, \cdots, a_\tau$ are rational integers.

If ρ is any root of $P(y) = 0$, all the roots are ρ^{t_j} $(j = 1, \cdots, \tau)$, and if u, v are integers, $\rho^u = \rho^v$ when and only when $u \equiv v \bmod m$.

If in any formula containing ρ it is desired to express everything in terms of m, it is convenient to replace ρ by the particular root $\exp(2\pi i/m)$.

Any rational function $A(\rho)$ of ρ is uniquely reducible to a polynomial in ρ of degree $\tau - 1$ with rational coefficients. If this polynomial is $R(\rho)$, we shall write

$$(3)\qquad A(\rho) \equiv R(\rho) \bmod P(\rho).$$

3. *Unreduced* $f(x)$. Write as definitions of $Q(y)$, $Q_i(y)$,

$$Q(y) = \prod_{i=1}^{s}(y - \rho^{r_i}), \qquad Q_i(y) = Q(y)/(y - \rho^{r_i}).$$

Denote by $Q'(z)$ the result of putting $y = z$ in the derivative $Q'(y)$ of $Q(y)$ with respect to y. Then $f(x)$ in (1) is

$$(4)\qquad f(x) = \sum_{i=1}^{s} \frac{k_i}{\rho^x - \rho^{r_i}} \cdot \frac{Q(\rho^x)}{Q_i(\rho^{r_i})}.$$

For $f(r_i) = k_i$, obviously, and $f(x)$ has the required periodicity mod m. We may write in a form more convenient for reduction to a polynomial in ρ^x,

$$(5)\qquad f(x) = Q(y) \sum_{i=1}^{s} \frac{k_i}{(y - \rho^{r_i})Q'(\rho^{r_i})}, \quad (y = \rho^x).$$

No $Q'(\rho^{r_i}) = 0$, since $Q(y)$ has no repeated root.

4. *Reduced* $f(x)$. At any stage of the following any exponent of ρ may be replaced by its least positive residue mod m, since $\rho^m = 1$. If m is even, $\rho^{m/2} = -1$, and further immediate reduction is possible. The coefficients of the several powers of y will in general be polynomials in ρ; these are reduced as in (3). Write

$$D(\rho) = \prod_{i=1}^{s} Q'(\rho^{r_i}), \qquad D(\rho)/Q'(\rho^{r_i}) = D_i(\rho).$$

Then (5) becomes

$$D(\rho)f(x) = \sum_{i=1}^{s} k_i D_i(\rho) Q_i(y). \tag{6}$$

In this the $D(\rho)$, $D_i(\rho)$ are polynomials in ρ with rational integral coefficients, and the $Q_i(y)$ are polynomials of degree $s-1$ in y whose coefficients are polynomials of the same kind as the $D(\rho)$, $D_i(\rho)$. We may assume that all polynomials in ρ in (6) have been reduced as indicated modulis $P(\rho)$, ρ^m-1 (or $\rho^{m/2}+1$ if m is even), so that all are now of degree $\leqq\tau-1$ in ρ. If $m=2$ the rest of the reduction is obvious. If $m>2$, then $\tau>1$. Multiply throughout by $D(\rho^{t_2})\cdots D(\rho^{t_\tau})$. The coefficient of $f(x)$ is then a symmetric function of the roots of $P(y)=0$, and hence is a rational integer, say r. The new right-hand member is now multiplied out, reductions by the two moduli being performed as convenient. The final result is

$$rf(x) = \sum_{i=0}^{s-1} R_i(\rho) y^i, \quad (y = \rho^x), \tag{7}$$

where the $R_i(\rho)$ are polynomials in ρ of degree $\leqq\tau-1$ whose coefficients are linear functions of $k_i, \cdots, k_s$ with rational integral coefficients, and r is a rational integer.

Equality being stronger than congruence, either of (5), (7) is a solution of

$$f(x) \equiv k_i \bmod m_i \quad \text{when} \quad x \equiv r_i \bmod m, \quad (i = 1, \cdots, s), \tag{8}$$

the m_i, k_i being now given constant integers, the m_i different from zero.

5. *Example.* Take $m=8$, $s=4$, $(r_1, r_2, r_3, r_4)=(1, 3, 5, 7)$, $(k_1, k_2, k_3, k_4)=(1,-1, -1, 1)$. The $f(x)$ then defined by (1) is the quadratic character $(2\,|x)$, x odd. Here (2) is $P(y)=y^4+1$, and $\rho^2=1$, $\rho^4=-1$. In §3 we have $Q(y)=P(y)$; hence we have also $Q'(y)=4y^3$, and reduction of (5) gives (7) in the form $2f(x)=\rho(\rho^2-1)\rho^x(\rho^{2x}-1)$. In trigonometric form this gives

$$f(x) = -2i^{x+1}\sin\frac{\pi}{4}\sin\frac{\pi x}{4},$$

where $i=(-1)^{1/2}$.

6. *A Special Reduction.* When $s=\tau$ (see §2) and $(r_1, \cdots, r_\tau) = (t_1, \cdots, t_\tau)$, the polynomials $P(y)$ in (2) and $Q(y)$ in §3 are

identical. In this case, which is of frequent occurrence, particularly in connection with power residues, a special reduction is sometimes useful.

Let $x \geqq 0$ be an integer. Then

$$\rho^x = f_0(x) + \rho f_1(x) + \cdots + \rho^{\tau-1} f_{\tau-1}(x), \tag{9}$$

where the $f_i(x)$ are uniquely determined rational integers. If x were <0, we should write $\rho^{-x} =. \rho^{hm-x}$, $h =$ the least positive integer such that $hm - x \geqq 0$, thus reducing this case to the former.

The τ sequences

$$f_i(x), \qquad (x = 0, 1, \cdots; i = 0, \cdots, \tau - 1), \tag{10}$$

have the characteristic equation $P(y) = 0$,

$$f_i(x + \tau) + a_1 f_i(x + \tau - 1) + \cdots + a_\tau f_i(x) = 0, \tag{11}$$

with the initial values

$$f_i(j) = \delta_{ij}, \qquad (i, j = 0, 1, \cdots, \tau - 1), \tag{12}$$

where $\delta_{ij} = 1$ if $i = j$, $\delta_{ij} = 0$ if $i \neq j$; whence the $f_i(x)$ can be calculated by recurrence. This is often shorter than division by $P(\rho)$.

The general solution of (11), for x restricted to integral values (not necessarily positive), is

$$f(z) = c_1 \rho^{t_1} + \cdots + c_\tau \rho^{t_\tau z}, \qquad (z = 0, \pm 1, \pm 2, \cdots).$$

Replacing z by $z + m$, we see that

$$f(z + m) = f(z), \tag{13}$$

since $\rho^m = 1$. Hence in particular the $f_i(x)$ have the period m. If m is even it follows in the same way that

$$f(z + m/2) = - f(z). \tag{14}$$

It is easily seen by a simple contradiction that $p = m, q = m/2$ are the least positive integers such that

$$f(z + p) = f(z), \; f(z + q) = - f(z).$$

Hence m is the true period in (13), and $m/2$ the true half period in (14).

California Institute of Technology