ON THE REPRESENTATION OF NUMBERS MODULO m*

BY E. D. RAINVILLE

Dirichlet and Kronecker† extended the notion of primitive root to the case of any composite modulus. The classical Kronecker-Dirichlet theorem may be stated as follows. *Let* $m=2^{\alpha_0}p_1^{\alpha_1}\cdots p_v^{\alpha_v}$, *where the p's are distinct odd primes. Determine* g_k, *a primitive root of* $p_k^{\alpha_k}$, *for* $k=1,2,\cdots,v$. *Form*

$$\lambda_k = g_k + p_k^{\alpha_k}\beta_k \equiv 1 \mod m/p_k^{\alpha_k},$$

and, if $\alpha_0>1$,

$$\lambda = -1 + 2^{\alpha_0}\beta \equiv 1 \mod m/2^{\alpha_0},$$

$$\lambda_0 = 5 + 2^{\alpha_0}\beta_0 \equiv 1 \mod m/2^{\alpha_0}.$$

Then, for $(n,m)=1$, *n is uniquely represented modulo m by*

$$n \equiv \lambda^i\lambda_0^{i_0}\prod_{k=1}^{v}\lambda_k^{i_k} \mod m,$$

where the exponents are restricted by the inequalities

$$0 \leqq i \leqq 1, \qquad 0 \leqq i_0 \leqq \phi(2^{\alpha_0-1}) - 1, \qquad 0 \leqq i_k \leqq \phi(p_k^{\alpha_k}) - 1.$$

If $\alpha_0\leqq 1$, λ *and* λ_0 *are not to be formed, hence* $i=i_0=0$ *automatically.*

In the course of another investigation a further extension to the case of general n (dropping the restriction $(n,m)=1$) became necessary. This is the object of the present note.

THEOREM. *Let* $m=2^{\alpha_0}p_1^{\alpha_1}\cdots p_v^{\alpha_v}$ *(p's distinct odd primes). Determine* g_k, *a primitive root‡ of* p_k^2, $k=1,2,\cdots,v$. *Form*

$$\lambda_k = g_k + p_k^{\alpha_k}\beta_k \equiv 1 \mod m/p_k^{\alpha_k}$$

and, if $\alpha_0>1$,

---

* Presented to the Society, March 18, 1933.

† Dickson, *History of the Theory of Numbers*, vol. 1, pp. 185, 192.

‡ The root g_k is then also a primitive root of p_k^n, $n>0$ (Dirichlet-Dedekind, *Zahlentheorie*, 4th ed., 1894, p. 334).

$$\lambda = -1 + 2^{\alpha_0}\beta \equiv 1 \mod m/2^{\alpha_0},$$
$$\lambda_0 = 5 + 2^{\alpha_0}\beta_0 \equiv 1 \mod m/2^{\alpha_0}.$$

Then any n is uniquely represented modulo m by

$$n \equiv 2^{\sigma_0}\lambda^{i}\lambda_0^{i_0} \prod_{k=1}^{v} p_k^{\sigma_k}\lambda_k^{i_k} \mod m, \tag{A}$$

where

$$0 \leqq \sigma_0 \leqq \alpha_0, \qquad 0 \leqq \sigma_k \leqq \alpha_k, \qquad (k = 1, 2, \cdots, v),$$

and the other exponents are subject to the restrictions that

if $\sigma_0 \geqq \alpha_0 - 1$, *then* $i = i_0 = 0$;
if $0 \leqq \sigma_0 \leqq \alpha_0 - 2$, *then* $0 \leqq i \leqq 1$ *and* $0 \leqq i_0 \leqq \phi(2^{\alpha_0-\sigma_0-1}) - 1$;
if $0 \leqq \sigma_k \leqq \alpha_k$, *then* $0 \leqq i_k \leqq \phi(p_k^{\alpha_k-\sigma_k}) - 1$,

for $k = 1, 2, \cdots, v$.

PROOF. In order to show that all numbers are represented uniquely by (A) we prove (1) that the number of such representations is m, and (2) that no two representations are congruent modulo m.

(1) The number of combinations of exponents σ_0, i, i_0 due to letting σ_0 assume all permissible values is evidently

$$1 + 1 + 2\cdot \sum_{\sigma_0=0}^{\alpha_0-2}\phi(2^{\alpha_0-\sigma_0-1}) = 1 + \phi(2) + \sum_{\sigma_0=0}^{\alpha_0-2}\phi(2^{\alpha_0-\sigma_0})$$
$$= \sum_{\sigma_0=0}^{\alpha_0}\phi(2^{\alpha_0-\sigma_0}) = 2^{\alpha_0}.$$

Similarly, for any $k = 1, 2, \cdots, v$, the number of combinations of exponents σ_k, α_k due to letting σ_k assume all permissible values is

$$\sum_{\sigma_k=0}^{\alpha_k}\phi(p_k^{\alpha_k-\sigma_k}) = p_k^{\alpha_k}.$$

Hence, combining these results, we have for T, the total number of representations,

$$T = 2^{\alpha_0}p_1^{\alpha_1} \cdots p_v^{\alpha_v} = m.$$

(2) The uniqueness is made to depend upon the Kronecker-Dirichlet theorem in the following manner. Suppose, with the restrictions of our theorem, that

$$2^{\sigma_0'}\lambda^{i}\lambda_0^{i_0}\prod_{k=1}^{v}p_k^{\sigma_k}\lambda_k^{i_k} \equiv 2^{\sigma_0'}\lambda^{i'}\lambda_0^{i_0'}\prod_{k=1}^{v}p_k^{\sigma_k'}\lambda_k^{i_k'} \quad \mathrm{mod}\ m.$$

Then, since λ, λ_0 and λ_k are relatively prime to m,

$$\sigma_0=\sigma_0', \qquad \sigma_k=\sigma_k', \qquad (k=1, 2, \cdots, v),$$

and we have

$$\text{(B)} \qquad \lambda^{i}\lambda_0^{i_0}\prod_{k=1}^{v}\lambda_k^{i_k} \equiv \lambda^{i'}\lambda_0^{i_0'}\prod_{k=1}^{v}\lambda_k^{i_k'} \ \mathrm{mod}\ 2^{\alpha_0-\sigma_0}\prod_{k=1}^{v}p_k^{\alpha_k-\sigma_k}.$$

Since λ_k is a primitive root of p_k^2, it is a primitive root of $p_k^{\alpha_k-\sigma_k}$. From the restrictions of the theorem, we conclude that $0\leqq i_k$, $i_k'\leqq\phi(p_k^{\alpha_k-\sigma_k})-1$. Further, $0\leqq i_0$, $i_0'\leqq\phi(2^{\alpha_0-\sigma_0-1})-1$, if only $\alpha_0-\sigma_0>1$. Again, if $\alpha_0-\sigma_0>1$, we know that $0\leqq i$, $i'\leqq 1$.

Thus all conditions of the Kronecker-Dirichlet theorem are satisfied in (B) for the modulus

$$2^{\alpha_0-\sigma_0}\prod_{k=1}^{v}p_k^{\alpha_k-\sigma_k} = (m/2^{\sigma_0})\prod_{k=1}^{v}p_k^{\sigma_k},$$

and the representation $\lambda^{i}\lambda_0^{i_0}\prod_{k=1}^{v}\lambda_k^{i_k}$ is a unique representation modulo $(m/2^{\sigma_0})\prod_{k=1}^{v}p_k^{\sigma_k}$, and, a fortiori, modulo m. Therefore, the representation (A) is unique modulo m.

THE UNIVERSITY OF COLORADO