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*

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

and, if $\alpha_0>1$,

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

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

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

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

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*

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

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).