des Tables dont on est redevable à quelques mathématiciens, c'est-à-dire pour les nombres à l'égard desquels ces méthodes sont inutiles, elles fatiguent la patience du calculateur le plus exercé, et qu'elles ne sont pour ainsi dire pas applicables à de plus grands nombres. (GAUSS, *Disquisitiones Arithmeticæ*, n° 329).

Nous allons exposer une méthode nouvelle qui permet de reconnaitre les nombres premiers très-grands, et de décomposer en leurs facteurs des nombres N très-grands, lorsque l'on connaît à l'avance la décomposition en ses facteurs premiers du nombre $N \pm 1$. Cette méthode a reçu l'approbation de MM. GENOCCHI et TCHEBICHEF, les illustres professeurs des Universités de Turin et de Saint-Pétersbourg, et je tiens à les remercier ici de la bienveillance avec laquelle ils ont accueilli mes premiers essais [1].

1. Si l'on désigne par $a, b, c, \ldots$, des nombres entiers, et par p un nombre premier, on déduit immédiatement du développement de la puissance p du polynome $a+b+c+\ldots$, la congruence

$$a^p+b^p+c^p+\ldots \equiv (a+b+c+\ldots)^p, \qquad (\text{Mod. } p),$$

de laquelle résulte, pour $a=b=c=\ldots,=1$, le théorème de FERMAT.

Si, maintenant, $a, b, c, \ldots$, désignent les racines d'une équation dans laquelle les coefficients sont entiers, et celui de la plus haute puissance de l'inconnue égal à l'unité, l'expression

$$a^{np}+b^{np}+c^{np}+\ldots - (a^n+b^n+c^n+\ldots)^p$$

désigne le produit par p d'une fonction symétrique entière des racines de l'équation, et, par suite, un multiple de p. On a donc encore, en représentant par S_q la somme des puissances $q^{\text{ièmes}}$ des racines de cette équation, la congruence

$$S_{np} \equiv S_n^p, \qquad (\text{Mod. } p),$$

et, par l'application du théorème de FERMAT,

$$S_{np} \equiv S_n, \qquad (\text{Mod. } p).$$

L'étude des diviseurs premiers de la fonction numérique S_n est fort importante; on a ainsi, en particulier, pour $n=1$, et $S_1=0$, comme dans l'équation

$$x^3 = x+1,$$

1 Voir les *Atti della Reale Accademia delle Scienze di Torino*, séance du 21 mai 1876.