22.

Démonstration de quelques théorèmes sur les nombres.

(Par Mr. *Stern* doct. en phil. à Goettingue.)

Dans un mémoire sur la théorie des nombres, inséré dans le T. 9. cah. 1. de ce journal, Mr. *Libri* a donné les deux congruences suivantes qu'il regarde comme renfermant un théorème exclusif et assez curieux sur les nombres premiers de la forme $6p+1$, savoir:

19. $$6p - \frac{6p.6p-1.6p-2}{1.2.3}3 + \frac{6p.6p-1.6p-2.6p-3.6-4}{1.2.3.4.5}3^2 - \ldots.$$
$$\ldots. \equiv 0 \pmod{6p+1},$$

20. $$6p-1 - \frac{6p-1.6p-2.6p-3}{1.2.3}3 + \frac{6p-1.6p-2.6p-3.6p-4.6p-5}{1.2.3.4.5}3^2 - \ldots.$$
$$\ldots. + 2^{6p-2} \equiv 0 \text{ *)} \pmod{6p+1}.$$

On peut démontrer ces théorèmes sans avoir recours à la théorie des nombres et montrer en même temps qu'ils sont contenus dans deux autres propositions plus générales et purement algébriques.

En effet, les deux racines imaginaires de l'équation

$$x^3 - 1 = 0$$

étant

$$= \frac{-1+\sqrt{-3}}{2} \text{ et } = \frac{-1-\sqrt{-3}}{2},$$

on a

$$a. \quad \left(\frac{-1+\sqrt{-3}}{2}\right)^{3m} = \left(-\frac{1}{2}\right)^{3m}.(1-\sqrt{-3})^{3m}$$
$$= \left(-\frac{1}{2}\right)^{3m}\left[1-3m\sqrt{-3} - \frac{3m.3m-1}{1.2}3 + \frac{3m.3m-1.3m-2}{1.2.3}3\sqrt{-3}\ldots\right] = 1,$$

$$b. \quad \left(\frac{-1-\sqrt{-3}}{2}\right)^{3m} = \left(-\frac{1}{2}\right)^{3m}(1+\sqrt{-3})^{3m}$$
$$= \left(-\frac{1}{2}\right)^{3m}\left[1+3m\sqrt{-3} - \frac{3m.3m-1}{1.2}3 - \frac{3m.3m-1.3m-2}{1.2.3}3\sqrt{-3}\ldots.\right] = 1,$$

en désignant par m un nombre entier quelconque.

En ajoutant les deux équations ($a.$) et ($b.$) on trouve

$$\left(-\frac{1}{2}\right)^{3m}\left[2 - 2.\frac{3m.3m-1}{1.2}3 + 2.\frac{3m.3m-1.3m-2}{1.2.3}3^2\ldots.\right] = 2,$$

*) Dans le mémoire cité on trouve -2^{6p-2}, mais c'est une erreur typographique.

ou bien

$$c.\quad 1-\frac{3m.3m-1}{1.2}3+\frac{3m.3m-1.3m-2.3m-3}{1.2.3.4}3^2\ldots.=2^{3m}.(-1)^{3m}.$$

En soustrayant l'équation (*b.*) de l'équation (*a.*) on obtiendra, après les réductions convenables, l'équation

$$d.\quad 3m-\frac{3m.3m-1.3m-2}{1.2.3}3+\ldots.=0.$$

On a aussi

$$e.\quad \left(\frac{-1+\sqrt{-3}}{2}\right)^{3m-1}=\frac{-2}{1-\sqrt{-3}}=$$

$$\left(-\frac{1}{2}\right)^{3m-1}\left[1-(3m-1)\sqrt{-3}-\frac{3m-1.3m-2}{1.2}3+\frac{3m-1.3m-2.3m-3}{1.2.3}3\sqrt{-3},\ldots\right],$$

$$f.\quad \left(\frac{-1-\sqrt{-3}}{2}\right)^{3m-1}=\frac{-2}{1+\sqrt{-3}}=$$

$$\left(-\frac{1}{2}\right)^{3m-1}\left[1+(3m-1)\sqrt{-3}-\frac{3m-1.3m-2}{1.2}3-\frac{3m-1.3m-2.3m-3}{1.2.3}3\sqrt{-3}\ldots.\right].$$

En ajoutant les équations (*e.*) et (*f.*) on trouve

$$\left(-\frac{1}{2}\right)^{3m-1}.2\left[1-\frac{3m-1.3m-2}{1.2}3\ldots.\right]=-1,$$

ou bien

$$g.\quad 1-\frac{3m-1.3m-2}{1.2}3\ldots.=(-1)^{3m}.2^{3m-2}.$$

En soustrayant l'équation (*e.*) de l'équation (*f.*), on trouve

$$h.\quad 3m-1-\frac{3m-1.3m-2.3m-3}{1.2.3}3\ldots.=(-1)^{3m-1}.2^{3m-2}.$$

En substituant dans les équations (*d.*) et (*h.*), $2p$ au lieu de m, on aura

$$i.\quad 6p-\frac{6p.6p-1.6p-2}{1.2.3}3+\ldots.=0,$$

$$k.\quad 6p-1-\frac{6p-1.6p-2.6p-3}{1.2.3}3\ldots.+2^{6p-2}=0$$

et l'on voit que ces équations contiennent les deux congruences citées comme des cas spéciaux.

Mr. *Libri* a déduit de la congruence (19.) le théorème connu que la congruence $x^2-3\equiv 0 \pmod{p}$ est toujours résoluble lorsque p est un nombre premier de la forme $12n+1$. En ayant égard à la forme des racines de l'équation

$$x^3-1=0,$$

on peut en déduire tous les cas dans lesquels les congruences

$$x-3\equiv 0 \pmod{p},\qquad x+3\equiv 0 \pmod{p}$$

sont résolubles, p désignant un nombre premier.

En effet parceque les racines de l'équation $x^4-1=0$ sont

$$=+1,\ =-1,\ =+\sqrt{-1},\ =-\sqrt{-1}$$

il faut que les racines de la congruence

$$x^4-1\equiv 0 \pmod{p}$$

soient $=+1,\ =-1,\ =+\sqrt{(mp-1)},\ =-\sqrt{(mp-1)}$.

Maintenant on sait que la congruence $x^4-1\equiv 0$ a quatre racines réelles ou seulement deux, selon que le nombre p est de la forme $4n+1$ ou de la forme $4n+3$. Ainsi il faut que dans le premier cas on ait

$$\sqrt{(mp-1)}=z$$

z désignant un nombre entier, ou

$$z^2\equiv -1 \pmod{p}.$$

Dans le second cas on ne peut jamais trouver un tel nombre. De là il suit *que le nombre* -1 *est un résidu ou un non-résidu quadratique du nombre premier* p *selon que ce nombre est de la forme* $4n+1$ ou de la forme $4n+3$.

Parceque l'équation $x^3-1=0$ a les trois racines

$$1,\ \frac{-1+\sqrt{3}}{2},\ \frac{-1-\sqrt{-3}}{2},$$

il faut que la congruence

$$x^3-1\equiv 0 \pmod{p}$$

ait les trois racines

$$-1,\ \frac{-1+\sqrt{(mp-3)}}{2},\ \frac{-1-\sqrt{(mp-3)}}{2}.$$

Mais cette congruence a trois racines réelles ou elle en a seulement une, selon que le nombre premier p est de la forme $3n+1$ ou de la forme $3n+2$. Ainsi dans le premier cas il faut qu'on ait

$$\sqrt{(mp-3)}=z$$

z désignant un nombre entier, ou bien

$$z^2\equiv -3 \pmod{p}.$$

Dans le second cas on ne peut jamais trouver un tel nombre, c'est-à-dire: *le nombre* -3 *est un résidu ou un non-résidu quadratique du nombre premier* p *selon que ce nombre est de la forme* $3n+1$ *ou de la forme* $3n+2$.

Maintenant on n'a qu'à combiner ce théorème avec le théorème précédent pour trouver toutes les propriétés des congruences

$$x^2-3\equiv 0 \pmod{p}, \qquad x^2+3\equiv 0 \pmod{p}.$$

Si le nombre p est de la forme $3n+1$ et que l'on désigne par f une

racine de l'équation

$$x^3 - 1 \equiv 0 \pmod{p},$$

on a

$$f \equiv \frac{-1 \pm \sqrt{(mp-3)}}{2},$$

ou

$$(2f+1)^2 \equiv -3 \pmod{p}$$

c'est-à-dire, que si l'on connait déjà le nombre f, on peut en déduire le nombre x qui satisfait à la congruence

$$x^2 \equiv -3 \pmod{p}$$

qu'on a déjà trouvé par d'autres voies (Voy. ce journ. T. 8. cah. 2. et T. 9. cah. 1.).

Goettingue le 12. Decembre 1833.