On some theorems in the theory of numbers.

By R. E. ALLARDICE, M.A.

The number of groups of n which may be selected from $2n$ is $2n(2n-1)\ldots(n+1)/n!$ But make the $2n$ into two groups of n, and select r out of the first and $n-r$ out of the second. This gives $[n(n-1)\ldots(n-r+1)/r!]+[n(n-1)\ldots(r+1)/(n-r)!]$ ways of thus making a group of n. Hence

$$* \; 2n(2n-1)\ldots(n+1)/n! = 1 + n^2 + [n(n-1)/2!]^2 + \ldots \qquad \ldots \qquad (1).$$

$$\therefore\; 2n(2n-1)\ldots(n+1)/n! - 2$$

$$= n^2\{1^2 + [(n-1)/2!]^2 + [(n-1)(n-2)/3!]^2 + \ldots\}$$

$$= n^2\{P_1^2 + P_2^2 + \ldots + P_{n-1}^2\} \text{ (say).}$$

We shall now show that $P_1^2 + P_2^2 + - - + P_{n-1}^2$ is divisible by n, if n be prime.

$P_r \equiv P_s$ (mod. n.), if $r+s=n$, but not otherwise. For if $P_r \equiv P_s$ $(r>s)$, then

$$(n-1)(n-2)\ldots(n-r+1)/r! - (n-1)(n-2)\ldots(n-s+1)/s! \equiv 0;$$

$$\therefore \frac{(n-1)(n-2)\ldots(n-s+1)}{s!}\left\{\frac{(n-s)(n-s-1)\ldots(n-r+1)}{(s+1)(s+2)\ldots\quad r} - 1\right\} \equiv 0;$$

$$\therefore (n-s)(n-\overline{s+1})(n-\overline{s+2})\ldots(n-\overline{r-1}) - (s+1)(s+2)\ldots r \equiv 0;$$

$$\therefore \quad \pm s(s+1)(s+2)\ldots(r-1) - (s+1)(s+2)\ldots r \equiv 0;$$

$$\therefore \quad -(s+1)(s+2)\ldots(r-1)(\mp s + r) \equiv 0;$$

and this is true if $r+s=n$ (otherwise obvious) and not in any other case. [If $r+s=n$, then $r-s=n-2s$, which is odd, and the lower sign is to be taken where the double sign is printed.]

It is obvious that $P_r + P_s$ is not divisible by n; and hence if we divide $P_1, P_2, \ldots P_{(n-1)/2}$ by n, we must get for remainders either 1 or $n-1$ and either 2 or $n-2$ and so on.

Now since $(n-r)^2 = n^2 - 2nr + r^2 \equiv r^2$ (mod. n), we must have

$$P_1^2 + P_2^2 + \ldots P_{(n-1)/2}^2 \equiv 1^2 + 3^2 + 5^2 \ldots + (n-2)^2$$

$$= n(n-1)(n-2)/6;$$

which is divisible by n if n be any prime except 2 or 3.

From this, and the identity (1), it follows that

$$(2n-1)(2n-2)\ldots(n+1) - (n-1)(n-2)\ldots 1 \equiv 0 \text{ (mod. } n^3).$$

---

* The use of this identity was suggested to me by Professor Tait.

We shall next show that $\left(1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n-1}\right)(n-1)!$ is divisible by n^2.*

We have

$$\left(1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n-1}\right)(n-1)!=\left(\frac{n}{1.(n-1)}+\frac{n}{2.(n-2)}+\ldots\right)(n-1)!$$

Hence we have to show thát $\left(\frac{1}{1.(n-1)}+\frac{1}{2.(n-2)}+\ldots\right)(n-1)!$ is exactly divisible by n.

Assume $(n-1)!/1.(n-1)=a_1$, $(n-1)!/2.(n-2)=a_2$, &c.

Then

$$\begin{aligned}(r+1)^2a_{r+1}-r^2a_r &= (r+1)^2(\overline{n-1}!)/(r+1)(n-r-1)-r^2(\overline{n-1}!)/r(n-r)\\ &= \{(r+1)/(n-r-1)-r/(n-r)\}(n-1)!\\ &= (n!)/(n-r)(n-r-1)\equiv 0 \pmod{n}.\\ \therefore\ (r+1)^2a_{r+1} &\equiv r^2a_r\\ &\equiv (r-1)^2a_{r-1}\\ &\quad \ldots\quad \ldots\quad \ldots\\ &\equiv 1^2.a_1\\ &\equiv 1 \qquad\qquad \text{(by Wilson's theorem).}\end{aligned}$$

Hence we may write

$$\begin{aligned}a_1 &= n\mu_1+1\\ 2^2a_2 &= n\mu_2+1\\ &\ldots\quad \ldots\quad \ldots\\ m^2a_m &= n\mu_m+1 \qquad\qquad \text{(where } m=(n-1)/2)\end{aligned}$$

$\therefore\ (m!)^2\Sigma a_r=\mathrm{P}.n+(m!)^2(1/1^2+1/2^2+\ldots+1/m^2)$.

Now, if we assume $(m\,!)/r\equiv a_r$, we may easily show that $a_r\pm a_s$ is not divisible by n, and hence that

$$a_1{}^2+a_2{}^2+\ldots+a_m^2\equiv 0 \pmod{n},$$

which proves the theorem.

Consider again the result

$$\mathrm{A}=(2n-1)(2n-2)\ldots(n+1)-(n-1)(n-2)\ldots 1\equiv 0 \pmod{n^3}.$$

This gives

$$\begin{aligned}\mathrm{A} &= (n+\overline{n-1})(n+\overline{n-2})\ldots(n+1)-(n-1)(n-2)\ldots 1\\ &= n^{n-1}+p_1n^{n-2}+\ldots+p_{n+3}n^2+p_{n-2}n,\end{aligned}$$

where $\quad p_{n-3}=(\overline{n-1}!)\Sigma(1/rs)(r+s)$

$\qquad\quad p_{n-2}=(\overline{n-1}!)\Sigma(1/r)$.

---

* Compare a paper by Mr Leudesdorf, in the *Proceedings of the Lond. Math. Soc.* for 1889, p. 199—a paper which I did not see till after the above was written.

Now p_{n-2} is divisible by n^2, and hence p_{n-3} is divisible by n.

This theorem may also be proved in the following manner:—
We have $2(\overline{n-1}!)\Sigma(1/rs)$

$$= \{(\overline{n-1}!)/1.2 + (\overline{n-1}!)/1.3 + \ldots + (\overline{n-1}!)/1.(n-1)\}(=P_1)$$
$$+ \{(\overline{n-1}!)/2.1 + (\overline{n-1}!)/2.3 + \ldots + (\overline{n-1}!)/2.(n-1)\}(=P_2)$$
$$+ \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

Now consider the terms of P_r, namely,

$$(\overline{n-1}!)/r.1, (\overline{n-1}!)/r.2, \ldots\ldots (\overline{n-1}!)/r.(r-1), (\overline{n-1}!)/r.(r+1), \text{ \&c.}$$

No two of these can be congruent; and

$$(\overline{n-1}!)/r.p + (\overline{n-1}!)r.(n-p) = n!/r.p.(n-p) \equiv 0 \pmod{n}.$$

Hence if we divide each of the terms of P_r by n, we get as remainders all the numbers 1, 2, $3\ldots n-1$, with the exception of that number which is complimentary to a_r where a_r

$$\equiv (\overline{n-1}!)/r.(n-r) \pmod{n}.$$

Hence the sum of all the remainders in $2\Sigma(n-1!)/rs$

$$= (n-1)(1+2+\ldots+\overline{n-1}) - 2(a_1 + a_2 + \ldots + a_{(n-1)})$$
$$= (n-1)^2 n/2 - 2\{1/1.(n-1) + 1/2.(n-2) + \ldots\}$$

which is divisible by n.

The theorem that the sum of the reciprocals of the numbers $1, 2, \ldots \overline{n-1}$, is divisible by n^2, when n is a prime, may be extended to the sum of the m^{th} powers of these numbers, where m is an integer, positive or negative.

Let $S_m = 1^m + 2^m + \ldots (n-1)^m$; it being understood that if m is negative $(=-l)$, the sum of the powers is to be multiplied by $(\overline{n-1}!)^l$, so that it may be made integral.

Since, when n is prime the equation

$$(x-1)(x-2)\ldots(x-\overline{n-1}) - x^{n-1} + 1 \equiv 0 \pmod{n}$$

has $(n-1)$ incongruent solutions, each co-efficient is divisible by n. Hence, if m is positive, S_m is divisible by n, unless m is a multiple of $(n-1)$.

Suppose now that m is an odd positive integer and $n \neq 2$; then

$$2\,S_m = 2\Sigma a^m = \Sigma(a^m + \overline{n-a}^m)$$
$$= \Sigma\{a^m + n^m - {}_mC_1 n^{m-1} a + \ldots + {}_mC_1 n a^{m-1} - a^m\}$$
$$\equiv n\Sigma_m C_1 a^{m-1} \equiv nmS_{m-1};$$

and $\qquad S_{m-1} \equiv 0 \pmod{n}$, unless $m-1$ is a multiple of $n-1$;

$\therefore \qquad S_m \equiv 0 \pmod{n^2}$, unless $m-1$ is a multiple of $n-1$;

and the theorem is true even in this last case if m is a multiple of n.

Now consider

$$S_{-m} = \{1 + 1/2^m + 1/3^m + \dots + 1/(n-1)^m\}(\overline{n-1}!)^m.$$

We have

$$\begin{aligned} 2\, S_{-m} &= (\overline{n-1}!)^m \Sigma\{1/r^m + 1/(n-r)^m\} \\ &= (\overline{n-1}!)^m \Sigma \frac{(n-r)^m + r^m}{r^m(n-r)^m} \\ &= (\overline{n-1}!)^m \Sigma \frac{n^m - {}_mC_1 n^{m-1} r \dots + {}_mC_1 n r^{m-1}}{r^m(n-r)^m} \\ &= (\overline{n-1}!)^m \Sigma \frac{Pn^2 + {}_mC_1 n}{r(n-r)^m}. \end{aligned}$$

We have thus to show that ${}_mC_1(\overline{n-1}!)^m\Sigma\{1/r(n-r)^m\}$ is divisible by n. We shall suppose, for the sake of clearness, that m is less than n; but the following method will be applicable, even if m be greater than n.

Assume $\quad (\overline{n-1}!)^m/\{(n-r)r^m\} \equiv a_r \pmod{n}$

$\therefore \quad (\overline{n-1}!)^m \equiv a_r(n-r)r^m$

$\therefore \quad a_r(n-r)r^m \equiv -1 \quad$ (by Wilson's theorem).

Now since $\quad (n-r)^{n-1} \equiv r^{n-1} \equiv 1$, we get

$$a_r \equiv -r^{n-m-1}(n-r)^{n-2}$$

$\therefore \quad a_r \equiv r^{n-m-1} r^{n-2} \pmod{n}$

$$\equiv r^{n-m-2}$$

Hence $\quad \Sigma a_r \equiv \Sigma r^{n-m-2}$

$$\equiv 0, \text{ if } n - m - 2 \neq 0.$$

It follows that S_{-m} is divisible by n_2, m being subject to the restriction $n - m - 2$ be not zero. If we remove the condition that m is to be less than n, we shall easily find that the general restriction as to the value of m, is that $m + 1$ must not be a multiple of $n - 1$.

In the paper referred to before in a footnote, Mr Leudesdorf considers the case where n is not prime and S_m denotes the sum of the m^{th} powers of the numbers less than n and prime to it. His method however cannot be considered rigorous, as it involves the use of divergent series.

Note on normals to conics.

By R. H. Pinkerton, M.A.

1. The following condition may be new; it does not appear in any of the books :—

The condition that the straight line