On Congruences. III.

By

Masazo Sono.

(Received May 23, 1918.)

In the previous paper entitled *On Congruences. II*[1], the author discussed the resolution of the ideals of a proper ring into factors prime to each other, and found the conditions for the unique resolvability of an ideal into prime factors, under the assumption that every ideal, distinct from the o-ideal, of the ring is of finite norm. The present paper is intended to show that the results relating to resolution, which have been obtained before, hold true also when the norms of the ideals are infinite, and then that the conditions for the unique resolvability are also substantially the same in this case.

For the sake of brevity the former papers[2] on congruences are here denoted by "Congr." and "Congr. II" respectively.

Resolution of an Ideal into Factors Prime to Each Other.

§ 1. Theorem: *Let $\mathfrak{B}$ be an ideal of a proper ring $\mathfrak{R}$, which is contained in another ideal $\mathfrak{A}$. If the quotient ring $\mathfrak{A}/\mathfrak{B}$ is a field, $\mathfrak{B}$ is equal to the product of $\mathfrak{A}$ and a maximal ideal prime to $\mathfrak{A}$.*

Herein $\mathfrak{A}$ is assumed to be distinct from $\mathfrak{R}$.

Take an element a of $\mathfrak{A}$ which does not belong to $\mathfrak{B}$, and the set of all the elements X which satisfy the congruence

$$aX \equiv 0 \qquad (\text{mod. } \mathfrak{B})$$

is an ideal of $\mathfrak{R}$, which we denote by $\mathfrak{M}$.

[1] These Memoirs, **3**, 113–149 (1918).

[2] On Congruences, these memoirs, **2**, 203 (1917).
On Congruences. II, these Memoirs, **3**, 113 (1918).

First evidently $\mathfrak{M}$ contains $\mathfrak{B}$, but contains no element of $\mathfrak{A}$ which does not belong to $\mathfrak{B}$; because the quotient $\mathfrak{A}/\mathfrak{B}$ is a field. And hence the cross-cut of $\mathfrak{A}$ and $\mathfrak{M}$ is $\mathfrak{B}$.

Secondly $\mathfrak{M}$ contains elements not belonging to $\mathfrak{A}$. For, since $\mathfrak{A}/\mathfrak{B}$ is a field, there exists in $\mathfrak{A}$ an element V, such that

$$AV \equiv A \qquad (\text{mod. } \mathfrak{B})$$

for every element A of $\mathfrak{A}$. And hence $a(V-1) \equiv 0$ (mod. $\mathfrak{B}$): so that the element $(V-1)$ belongs to $\mathfrak{M}$, while evidently not belonging to $\mathfrak{A}$.

Thirdly $\mathfrak{M}$ is prime to $\mathfrak{A}$. For, if the product aR, R being an element of $\mathfrak{R}$, belongs to $\mathfrak{M}$, it must belong to $\mathfrak{B}$; because aR is contained in $\mathfrak{A}$ at the same time. Therefore the ideal consisting of the elements Y for which $aY \equiv 0$ (mod. $\mathfrak{M}$) coincides with $\mathfrak{M}$. But, since the cross-cut of $\mathfrak{A}$ and $\mathfrak{M}$ is $\mathfrak{B}$, the quotient rings $(\mathfrak{A}, \mathfrak{M})/\mathfrak{M}$ and $\mathfrak{A}/\mathfrak{B}$ are of the same type [by Congr. § 11, theorem], while $\mathfrak{A}/\mathfrak{B}$ is a field. Therefore, if $\mathfrak{M}$ were not prime to $\mathfrak{A}$, namely if $(\mathfrak{A}, \mathfrak{M})$ were distinct from $\mathfrak{R}$, the ideal consisting of the elements Y for which $aY \equiv 0$ (mod. $\mathfrak{M}$) would contain elements not belonging to $(\mathfrak{A}, \mathfrak{M})$, as can similarly be shown. This contradicts the fact that it coincides with $\mathfrak{M}$. Therefore $\mathfrak{M}$ must be prime to $\mathfrak{A}$.

Lastly $\mathfrak{M}$ is maximal; because $(\mathfrak{A}, \mathfrak{M})/\mathfrak{M}$ is a field, while $(\mathfrak{A}, \mathfrak{M}) = \mathfrak{R}$.

Thus $\mathfrak{B}$ is the cross-cut of $\mathfrak{A}$ and the maximal ideal $\mathfrak{M}$ prime to $\mathfrak{A}$, and hence equal to the product of $\mathfrak{A}$ and $\mathfrak{M}$ [by Congr. § 5, theorem].

§ 2. THEOREM: *Let*

$$\mathfrak{R}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n \qquad (n \geqq 2)$$

be a chief-composition-series of a proper ring $\mathfrak{R}$, *with the last term* $\mathfrak{A}_n$. *Then, if any one of the quotient rings*

$$\frac{\mathfrak{A}_1}{\mathfrak{A}_2}, \frac{\mathfrak{A}_2}{\mathfrak{A}_3}, \ldots, \frac{\mathfrak{A}_{n-1}}{\mathfrak{A}_n}$$

derived from the series is a field, the ideal $\mathfrak{A}_n$ *is resolvable into two factors prime to each other. Conversely, if* $\mathfrak{A}_n$ *is resolvable into factors prime to each other, at least one of the quotient rings is a field.*

Proof. If the quotient ring $\mathfrak{A}_{n-1}/\mathfrak{A}_n$ is a field, the theorem has just been proved in the previous theorem.

We now suppose that $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is a field, but that none of the following:

$$\frac{\mathfrak{A}_{i+1}}{\mathfrak{A}_{i+2}},\ \frac{\mathfrak{A}_{i+2}}{\mathfrak{A}_{i+3}},\ \ldots,\ \frac{\mathfrak{A}_{n-1}}{\mathfrak{A}_n} \qquad (i < n-1)$$

are fields. Then, by the previous theorem, we have

$$\mathfrak{A}_{i+1} = \mathfrak{A}_i\mathfrak{M},$$

where $\mathfrak{M}$ is a maximal ideal prime to $\mathfrak{A}_i$. And the square of $\mathfrak{A}_{i+j}$ is contained in $\mathfrak{A}_{i+j+1}$ $(j \geqq 1)$ [*cf.* Congr., § 20]; and hence $\mathfrak{A}_{i+1}^{2^{n-i-1}}$ is contained in $\mathfrak{A}_n$. So that we have

$$\begin{aligned} \mathfrak{A}_n &= (\mathfrak{A}_n, \mathfrak{A}_{i+1}^e), \text{ where } e=2^{n-i-1} \\ &= (\mathfrak{A}_n, \mathfrak{A}_i^e\mathfrak{M}^e) \\ &= (\mathfrak{A}_n, \mathfrak{A}_i^e)(\mathfrak{A}_n, \mathfrak{M}^e) \qquad \text{[by Congr. II, §6, theorem];} \end{aligned}$$

because from $(\mathfrak{A}_i, \mathfrak{M})=\mathfrak{R}$, it follows that $(\mathfrak{A}_i^e, \mathfrak{M}^e)=\mathfrak{R}$ [by Congr. II, § 4, Cor.].

But, since evidently $\mathfrak{A}_n$ is contained in both $\mathfrak{A}_i$ and $\mathfrak{M}$, the ideals $(\mathfrak{A}_n, \mathfrak{A}_i^e)$ and $(\mathfrak{A}_n, \mathfrak{M}^e)$ are contained in $\mathfrak{A}_i$ and $\mathfrak{M}$ respectively, and moreover are evidently prime to each other. Therefore $\mathfrak{A}_n$ is resolvable into two factors prime to each other, neither of which is $\mathfrak{R}$.

Next, to prove the converse, suppose that

$$\mathfrak{A}_n = \mathfrak{L}\mathfrak{M},$$

where $\mathfrak{L}$ and $\mathfrak{M}$ are ideals prime to each other. Since $\mathfrak{A}_1$ is maximal, either $\mathfrak{L}$ or $\mathfrak{M}$ or both must be prime to $\mathfrak{A}_1$; because otherwise $\mathfrak{L}$ and $\mathfrak{M}$ would be contained in $\mathfrak{A}_1$, contrary to our assumption that they are prime to each other. And hence we may suppose that $\mathfrak{L}$ is prime to $\mathfrak{A}_1$. Then $\mathfrak{L}$ is also prime to the powers of $\mathfrak{A}_1$ [Congr. II, § 4, Cor.], and hence $\mathfrak{L}$, and consequently the ideal $\mathfrak{A}_n$ which is contained in $\mathfrak{L}$, contains no power of $\mathfrak{A}_1$. But, if none of the quotient rings were fields, the ideal $\mathfrak{A}_n$ would contain the power $\mathfrak{A}_1^{2^{n-1}}$ [*cf.* Congr. § 20]. Therefore at least one of the quotient rings is a field.

§ 3. If one of the quotient rings considered above, say $\mathfrak{A}_i/\mathfrak{A}_{i+1}$, is a field, no powers of $\mathfrak{A}_1$ are contained in $\mathfrak{A}_n$. For, no powers of an element of $\mathfrak{A}_i$ which does not belong to $\mathfrak{A}_{i+1}$ are contained in $\mathfrak{A}_{i+1}$, and hence no powers of $\mathfrak{A}_i$ in $\mathfrak{A}_{i+1}$. And moreover $\mathfrak{A}_n$ contains no powers of a maximal ideal distinct from $\mathfrak{A}_1$; because $\mathfrak{A}_1$ is prime to the powers of a maximal ideal distinct from itself [Congr. II, § 4, Cor.], while containing $\mathfrak{A}_n$.

On the contrary, if none of the quotient rings are fields, $\mathfrak{A}_n$ contains a power of $\mathfrak{A}_1$. Therefore the last theorem may be rewritten as follows:

An ideal $\mathfrak{A}$ of a proper ring is or is not resolvable into factors prime to each other, according as it does not or does contain a power of a maximal ideal. (Herein it is assumed that there exists a chief-composition-series with the last term $\mathfrak{A}$).

§ 4. THEOREM: *If the set of quotient rings derived from a chief-composition-series of a proper ring $\mathfrak{R}$, which has a given ideal $\mathfrak{A}$ for the last term, contains ν fields, the ideal $\mathfrak{A}$ can be expressed as the proproduct of ν ideals which contain powers of distinct maximal ideals respectively. And the maximal ideals containing $\mathfrak{A}$ are just ν in number.*

Proof. Let

$$(1) \qquad \mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\ \ldots,\ \mathfrak{A}_n$$

be a chief-composition-series of a proper ring $\mathfrak{R}$. We are to prove that, if just ν of the quotient rings

$$(2) \qquad \frac{\mathfrak{R}}{\mathfrak{A}_1},\ \frac{\mathfrak{A}_1}{\mathfrak{A}_2},\ \ldots,\ \frac{\mathfrak{A}_{n-1}}{\mathfrak{A}_n}$$

are fields, the ideal $\mathfrak{A}_n$ is resolvable into the product of ν ideals which contain powers of distinct maximal ideals respectively.

Since $\mathfrak{R}$ is proper, the quotient $\mathfrak{R}/\mathfrak{A}_1$ is a field. Therefore the set of quotient rings contains at least one field. If set (2) contains a single field, namely $\mathfrak{R}/\mathfrak{A}_1$, evidently $\mathfrak{A}_n$ contains a power of the maximal ideal $\mathfrak{A}_1$.

Next, suppose that there are in (2) just two fields, say $\mathfrak{R}/\mathfrak{A}_1$ and $\mathfrak{A}_i/\mathfrak{A}_{i+1}$. Then, as shown in § 2, we have

$$\mathfrak{A}_{i+1} = \mathfrak{A}_i\mathfrak{M},$$

and

$$\mathfrak{A}_n = (\mathfrak{A}_n, \mathfrak{A}_i^e)(\mathfrak{A}_n, \mathfrak{M}^e) \qquad [e = 2^{n-i-1}],$$

where $\mathfrak{M}$ is a maximal ideal prime to $\mathfrak{A}_i$. But, since none of the quotient rings $\frac{\mathfrak{A}_1}{\mathfrak{A}_2}, \frac{\mathfrak{A}_2}{\mathfrak{A}_3}, \ldots, \frac{\mathfrak{A}_{i-1}}{\mathfrak{A}_i}$ are fields, the ideal $\mathfrak{A}_i$ contains a power of $\mathfrak{A}_1$. Therefore both factors of $\mathfrak{A}_n$ contain powers of the distinct maximal ideals, $\mathfrak{A}_1$ and $\mathfrak{M}$, respectively. So that the theorem is true when $\nu=2$.

To proceed by induction, assume that the first part of the theorem is true when the set of quotient rings derived from a chief-composition-series contains $\nu-1$ fields, and that set (2) contains ν fields. Let us suppose that $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is a field, but none of the quotient rings

$$\frac{\mathfrak{A}_{i+1}}{\mathfrak{A}_{i+2}},\ \frac{\mathfrak{A}_{i+2}}{\mathfrak{A}_{i+3}},\ \dots,\ \frac{\mathfrak{A}_{n-1}}{\mathfrak{A}_n} \qquad (i \leqq n-1)$$

are fields. Then the set of quotient rings derived from the chief-composition-series

$$\mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\ \dots,\ \mathfrak{A}_i$$

contains just $(\nu-1)$ fields. Hence, by assumption, $\mathfrak{A}_i$ is resolvable as follows:

$$\mathfrak{A}_i = \mathfrak{M}_1\mathfrak{M}_2 \dots \mathfrak{M}_{\nu-1},$$

where $\mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_{\nu-1}$ are ideals containing powers of distinct maximal ideals respectively. And also, by § 2, theorem, we have

$$\mathfrak{A}_n = (\mathfrak{A}_n, \mathfrak{M}^e)(\mathfrak{A}_n, \mathfrak{A}_i^e) \qquad [e = 2^{n-i-1}],$$

where $\mathfrak{M}$ is a maximal ideal prime to $\mathfrak{A}_i$. But

$$(\mathfrak{A}_n, \mathfrak{A}_{i,}^e) = (\mathfrak{A}_n, \mathfrak{M}_1^e)(\mathfrak{A}_n, \mathfrak{M}_2^e) \dots (\mathfrak{A}_n, \mathfrak{M}_{\nu-1}^e),$$

since $\mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_{\nu-1}$ are prime to one another [*cf.* Congr. II, §§ 4, 6]. Therefore we have

$$\mathfrak{A}_n = (\mathfrak{A}_n, \mathfrak{M}^e)(\mathfrak{A}_n, \mathfrak{M}_1^e)(\mathfrak{A}_n, \mathfrak{M}_2^e) \dots (\mathfrak{A}_n, \mathfrak{M}_{\nu-1}^e),$$

which shows that $\mathfrak{A}_n$ is resolvable into ν factors respectively containing powers of distinct maximal ideals. Thus the former part of the theorem must hold true also when the number of fields contained in (2) is ν. It is therefore universally true.

Next, to prove the latter part, we suppose that set (2) contains just ν fields. Then we have

$$\mathfrak{A}_n = \mathfrak{L}_1\mathfrak{L}_2 \dots \mathfrak{L}\ ,$$

where $\mathfrak{L}_1, \mathfrak{L}_2 \dots, \mathfrak{L}_\nu$ are ideals respectively containing powers of distinct maximal ideals. If $\mathfrak{P}$ be a maximal ideal of $\mathfrak{R}$, which contains $\mathfrak{A}_n$, it must contain one of the $\mathfrak{L}$'*s*; because otherwise $\mathfrak{P}$ would be prime to all the $\mathfrak{L}$'*s* and consequently to their product $\mathfrak{A}_n$. And hence suppose that $\mathfrak{P}$ contains $\mathfrak{L}_1$ while $\mathfrak{L}_1$ contains a power of maximal ideal $\mathfrak{P}_1^d$. Then we have $\mathfrak{P}=\mathfrak{P}_1$; because otherwise $\mathfrak{P}$ would be prime to $\mathfrak{P}_1^d$, and consequently to $\mathfrak{L}_1$. Therefore the maximal ideals containing $\mathfrak{A}_n$ are ν in number.

§ 5. The resolution of an ideal, as stated in the last article, is possible, in a single way, viz.

THEOREM: *Every ideal $\mathfrak{A}$ of a proper ring, which contains no powers of a maximal ideal, may be expressed as the product of a finite number of ideals which contain powers of distinct maximal ideals respectively; and this can be done in one way only.* (Herein it is assumed that there exists a chief-composition-series with the last term $\mathfrak{A}$.)

The former part has already been proved, and hence it suffices to prove the latter. Resolve $\mathfrak{A}$ into factors as follows:

$$\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2 \dots \mathfrak{A}_\nu,$$

where $\mathfrak{A}_1, \mathfrak{A}_2. \dots, \mathfrak{A}_\nu$ are ideals containing powers of distinct maximal ideals $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_\nu$ respectively. Then a maximal ideal containing $\mathfrak{A}$ must be one of the following: $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_\nu$, as shown in the last article.

So that if two resolutions are possible, the maximal ideals, each of which contains one of the factors, are the same in both. And hence the only admissible supposition is

$$\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2 \dots \mathfrak{A}_\nu = \mathfrak{A}_1' \mathfrak{A}_2' \dots \mathfrak{A}_\nu',$$

where $\mathfrak{A}_i$ and $\mathfrak{A}_i'$ are ideals containing powers of the same maximal ideal $\mathfrak{P}_i$, $(i = 1, 2, \dots, \nu)$. Since $\mathfrak{A}_1'$ contains a power of $\mathfrak{P}_1$, it is prime to all of the ideals $\mathfrak{A}_2, \mathfrak{A}_3, \dots, \mathfrak{A}_\nu$ and consequently to their product [Congr. II, §4]; similarly $\mathfrak{A}_1$ is prime to the product $\mathfrak{A}_2'\mathfrak{A}_3' \dots \mathfrak{A}_\nu'$. Therefore we have

$$(\mathfrak{A}_1\mathfrak{A}_1', \mathfrak{A}_1\mathfrak{A}_2 \dots \mathfrak{A}_\nu) = \mathfrak{A}_1(\mathfrak{A}_1', \mathfrak{A}_2\mathfrak{A}_3 \dots \mathfrak{A}_\nu) = \mathfrak{A}_1,$$

$$(\mathfrak{A}_1'\mathfrak{A}_1, \mathfrak{A}_1'\mathfrak{A}_2' \dots \mathfrak{A}_\nu') = \mathfrak{A}_1'(\mathfrak{A}_1, \mathfrak{A}_2'\mathfrak{A}_3' \dots \mathfrak{A}_\nu') = \mathfrak{A}_1',$$

while $\mathfrak{A}_1\mathfrak{A}_2 \dots \mathfrak{A}_\nu = \mathfrak{A}_1'\mathfrak{A}_2' \dots \mathfrak{A}_\nu'$. Hence $\mathfrak{A}_1 = \mathfrak{A}_1'$. Taking $\mathfrak{A}_i$ and $\mathfrak{A}_i'$ for $\mathfrak{A}_1$ and $\mathfrak{A}_1'$, similarly we can show that $\mathfrak{A}_i = \mathfrak{A}_i'$. So that the two resolutions are identical.

§ 6. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two ideals of a proper ring $\mathfrak{R}$. If $\mathfrak{R}$ possesses chief-composition-series, one containing $\mathfrak{A}$, and the other $\mathfrak{B}$ for the last term, the maximal ideals which contain either $\mathfrak{A}$ or $\mathfrak{B}$ or both are finite in number, as shown already; hence let $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_\nu$ be the distinct maximal ideals which contain $\mathfrak{A}$, and $\mathfrak{Q}_1, \mathfrak{Q}_2, \dots, \mathfrak{Q}^\mu$ those which contain $\mathfrak{B}$. And also $\mathfrak{A}$ and $\mathfrak{B}$ are resolvable as follows:

$$\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2 \dots \mathfrak{A}_\nu,$$

$$\mathfrak{B} = \mathfrak{B}_1\mathfrak{B}_2 \dots \mathfrak{B}_\mu,$$

where $\mathfrak{A}_1, \ldots, \mathfrak{A}_\nu, \mathfrak{B}_1, \ldots, \mathfrak{B}$ are ideals which contain powers of $\mathfrak{P}_1, \ldots, \mathfrak{P}_\nu, \mathfrak{Q}_1, \ldots, \mathfrak{Q}_\mu$ respectively.

Of these maximal ideals, if the ones which contain both $\mathfrak{A}$ and $\mathfrak{B}$ are $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_\lambda$, we have

$$(\mathfrak{A}, \mathfrak{B}) = (\mathfrak{A}_1, \mathfrak{B}_1)(\mathfrak{A}_2, \mathfrak{B}_2)\ldots(\mathfrak{A}_\lambda, \mathfrak{B}_\lambda),$$

which can be proved entirely in the same way as in Congr. II, § 23.

It is evident, from the last theorem, that if $\mathfrak{A}$ contains $\mathfrak{B}$ then $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_\nu$ contain $\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_\nu$ respectively.

If, moreover, there is no ideal such that it contains $\mathfrak{P}_i^2$ and is distinct from $\mathfrak{P}_i$ and $\mathfrak{P}_i^2$, the ideals $\mathfrak{A}_i$ and $\mathfrak{B}_i$ are powers of $\mathfrak{P}_i$ [Congr. II, § 10], while $\mathfrak{A}_i$ contains $\mathfrak{B}_i$. So that $\mathfrak{A}_i$ divides $\mathfrak{B}_i$. Hence we have the

THEOREM: *Let $\mathfrak{R}$ be a proper ring such that, corresponding to a given ideal $(\neq 0)$, it possesses a chief-composition-series containing the ideal for the last term, and $\mathfrak{A}$ an ideal of $\mathfrak{R}$. If an ideal of $\mathfrak{R}$ which contains the square of a maximal ideal $\mathfrak{P}$ containing $\mathfrak{A}$ is either $\mathfrak{P}$ or $\mathfrak{P}^2$, then (i) $\mathfrak{A}$ is resolvable into the product of maximal ideals; (ii) $\mathfrak{A}$ divides the ideals of $\mathfrak{R}$ which are contained in $\mathfrak{A}$.*

Conditions for the Unique Resolvability of an Ideal into Prime Factors.

§ 7. In Congr. II, § 26 we defined prime and composite ideals, and made a few remarks about them. We give the same definition for them also in the present case; namely an ideal $\mathfrak{A}$ of a proper ring $\mathfrak{R}$, which is different from $\mathfrak{R}$, is called a prime ideal, if it has no other divisors distinct from $\mathfrak{R}$ and $\mathfrak{A}$: if otherwise, it is said to be composite. Then similarly we get the same results:

Let $\mathfrak{P}$ be a maximal ideal of a proper ring $\mathfrak{R}$. Then there are four cases to consider.

(1) Suppose that $\mathfrak{P}^2 = \mathfrak{P}$. $\mathfrak{P}$ apparently seems composite, but shall be considered as prime also here, because of having no other divisors distinct from $\mathfrak{R}$ and $\mathfrak{P}$. And evidently it divides the ideals of $\mathfrak{R}$ which are contained in it [by the last theorem].

(2) If $\mathfrak{P}^2 =$ the o-ideal, the ideals, except the o-ideal, are all prime.

(3) Suppose that $\mathfrak{P}^2 \neq 0$, and that there are ideals of $\mathfrak{R}$, distinct from $\mathfrak{P}$ and $\mathfrak{P}^2$, which contain $\mathfrak{P}^2$. Then such ideals are all prime.

Therefore the ideals of $\mathfrak{R}$ which are distinct from $\mathfrak{P}^2$ and contain $\mathfrak{P}^2$ are all prime.

(4) If there is no ideal such that it contains $\mathfrak{P}^2$ and is distinct from $\mathfrak{P}$ and $\mathfrak{P}^2$, then $\mathfrak{P}$ is prime, but the ideals of $\mathfrak{R}$ which are contained in $\mathfrak{P}$ are all composite [by the last theorem].

§ 8. To find the conditions for the unique resolvability of an ideal into prime factors, first we set the same convention as in Congr. II; namely, when $\mathfrak{P}^a = \mathfrak{P}^{a+1}$, $\mathfrak{P}$ being a prime ideal, the ideal $\mathfrak{P}^a$ is considered as not uniquely resolvable, even if divisible by no other prime ideals distinct from $\mathfrak{P}$.

Let $\mathfrak{R}$ be a proper ring subject to the following conditions:

(1) The product of two elements of $\mathfrak{R}$ is not equal to 0, unless at least one of the factors is equal to 0;

(2) Corresponding to any ideal $\mathfrak{A}$, distinct from the 0-ideal, of $\mathfrak{R}$, there exists a chief-composition-series of $\mathfrak{R}$ which contains $\mathfrak{A}$ for the last term.

Then we have the

THEOREM: *In order that every composite ideal of the ring $\mathfrak{R}$ may be uniquely resolvable into prime factors, it is necessary and sufficient that for every maximal ideal $\mathfrak{P}$ of $\mathfrak{R}$ the following conditions should be satisfied:*

(i) *An ideal of $\mathfrak{R}$ which contains $\mathfrak{P}^2$ is either $\mathfrak{P}$ or $\mathfrak{P}^2$;*

(ii) $\mathfrak{P}^e \neq \mathfrak{P}^{e+1}$ *for every exponent e.*

To prove the necessity of the conditions we assume that every composite ideal is uniquely resolvable into prime factors; and let $\mathfrak{P}$ be a maximal ideal of $\mathfrak{R}$. Then, by condition (1) for the ring, $\mathfrak{P}^2$ is never the 0-ideal, and hence, by condition (2), there is a chief-composition-series containing $\mathfrak{P}^2$ for the last term. And moreover $\mathfrak{P}^2$ must be distinct from $\mathfrak{P}$; because otherwise the resolution of a power of $\mathfrak{P}$ would not be unique according to our convention. Therefore a chief-composition-series of $\mathfrak{R}$ which contains $\mathfrak{P}^2$ for the last term consists either of three terms or of more than three terms. Namely the series is either

$$\mathfrak{R},\ \mathfrak{P},\ \mathfrak{P}^2,$$

or

$$\mathfrak{R},\ \mathfrak{P},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\ \ldots,\ \mathfrak{A}_n,\ \mathfrak{P}^2 \qquad (n \geqq 1).$$

If the latter case happened, the $\mathfrak{A}$'s would be all prime, as stated in the last article, and hence either $\mathfrak{P}^2$ or $\mathfrak{P}^3$ or both would be resolvable into prime factors in at least two ways, as seen from the results obtained in Congr. II, §§ 11–15. Therefore there is no ideal, distinct from $\mathfrak{P}$ and $\mathfrak{P}^2$, such that it contains $\mathfrak{P}^2$ and consequently is contained in $\mathfrak{P}$.

Condition (ii) is evidently necessary by our convention.

Next, to prove the sufficiency of the conditions we assume that they are satisfied. Then the maximal ideals are prime, but the others are all composite [§7, (4)]; and also an ideal is resolvable into the product of maximal ideals [§ 6, theorem]. Therefore a composite ideal $\mathfrak{A}$ may be reduced to the form

$$\mathfrak{P}_1^{e_1}\,\mathfrak{P}_2^{e_2}\ldots\,\mathfrak{P}_\nu^{e_\nu},$$

where $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_\nu$ are distinct prime ideals.

It is clear that a prime ideal dividing $\mathfrak{A}$ must be one of the $\mathfrak{P}$'*s*; because the prime ideal is maximal, and a maximal ideal distinct from all the $\mathfrak{P}$'*s* is prime to the product of their powers and consequently to $\mathfrak{A}$ [Congr. II, § 4]. And also is it clear that if two resolutions are possible the same prime ideals must occur in both; because otherwise the prime factors occurring in one only would be prime to $\mathfrak{A}$ [Congr. II, §4]. So that the only admissible supposition is

$$\mathfrak{P}_1^{e_1}\,\mathfrak{P}_2^{e_2}\ldots\,\mathfrak{P}_\nu^{e_\nu} = \mathfrak{P}_1^{e_1'}\,\mathfrak{P}_2^{e_2'}\ldots\,\mathfrak{P}_\nu^{e_\nu'}.$$

And then, by the theorem of § 5, we have

$$\mathfrak{P}_i^{e_i} = \mathfrak{P}_i^{e_i'} \qquad (i = 1, 2, \ldots, \nu),$$

whence, by condition (ii), we have

$$e_i = e_i' \qquad (i = 1, 2, \ldots, \nu).$$

So that the two resolutions are identical,

May, 1918.