Chinese remainder theorem

**Theorem:** Suppose $R$ is a non-zero commutative ring. Let $A_1, \ldots, A_n$ be a finite set of ideals of $R$.

1. The natural ring homomorphism

$$
\phi : R \rightarrow \bigoplus_{i=1}^{n} R/A_i
$$

has kernel $\bigcap_{i=1}^{n} A_i$.

2. Suppose that the $A_i$ are comaximal, in the sense that the ideal $A_i + A_j$ generated by $A_i$ and $A_j$ is all of $R$ if $i \neq j$. Then $\phi$ in part (1) is surjective, and

$$
\prod_{i=1}^{n} A_i = \bigcap_{i=1}^{n} A_i.
$$

The left side of this equality is the $R$-ideal generated by all products of the form $\prod_{i=1}^{n} a_i$ with $a_i \in A_i$. 

1
**Proof:** Part (1) is clear, so we now suppose the $A_i$ are comaximal.

The statement that $\phi$ is surjective is equivalent to the following assertion. Suppose $c_j \in R$ is given for each $i = 1, \ldots, n$. Then there is a solution $c \in R$ to the system of congruences

$$c \equiv c_i \mod A_i \quad \text{for} \quad i = 1, \ldots, n$$

To solve this system of congruences, we claim it will suffice to find for each $i$ an element $t_i \in R$ such that

$$t_i \equiv 1 \mod A_i$$

and

$$t_i \equiv 0 \mod A_j \quad \text{for} \quad j \neq i.$$ 

Given such $t_i$, we let

$$c = \sum_{i=1}^{n} t_i c_i.$$ 

Mod $A_j$, only the term $t_j c_j \equiv c_j \mod A_j$ is non-zero on the right, so $c$ solves the congruences.
We now produce the $t_i$.

For each $i \neq j$ there then exists $x_{i,j} \in A_i$ and $y_{i,j} \in A_j$ such that

$$x_{i,j} + y_{i,j} = 1$$

since $A_i + A_j = 1$. Fix $i$. We then have

$$1 = \prod_{\text{all } j \neq i} (x_{i,j} + y_{i,j}) = u_i + t_i \quad (*)$$

where

$$t_i = \prod_{j \neq i} y_{i,j} \in \prod_{j \neq i} A_j \quad (**$$

and $u_i \in A_i$ is the sum of all the other terms which come up when we expand the above product. Each of these other terms lies in $A_i$ because they involve at least one factor coming from $A_i$.

Reading $(*)$ and $(**)$ mod each of the $A_l$ shows $t_i$ has the properties we want.
It remains to show

\[ \prod_{i=1}^{n} A_i = \cap_{i=1}^{n} A_i. \]

The fact that the left side is contained in the right is clear, since the \( A_i \) are ideals.

Now suppose \( c \in \cap_{i=1}^{n} A_i \). We have

\[ c = c \cdot 1 = c \cdot (u_1 + t_1) = c \cdot u_1 + c \cdot t_1 \quad (*) \]

By construction, \( t_1 \in \prod_{j>1} A_j \) so since \( c_1 \in A_1 \),

\[ c \cdot t_1 \in \prod_{\text{all } i} A_i \quad (**) \]

We know \( c \in \cap_{i>1} A_i = \prod_{i>1} A_i \) by induction on \( n \). Since \( u_1 \in A_1 \) we get

\[ c \cdot u_1 \in \prod_{\text{all } i} A_i \quad (***) \]

Putting together \((*)\), \((***)\) and \((***)\) shows

\[ c \in \prod_{\text{all } i} A_i \]

so we’re done.
Example: If $R = \mathbb{Z}$, one can sometimes find an quicker construction of the $t_i$. For example, to solve the system of congruences
\[ c \equiv 1 \quad \text{mod} \quad (2) \]
\[ c \equiv 3 \quad \text{mod} \quad (7) \]
\[ c \equiv 5 \quad \text{mod} \quad (11) \]
one lets
\[ c = 1 \cdot t_2 + 3 \cdot t_7 + 5 \cdot t_{11} \]
for the appropriate $t_2$, $t_7$ and $t_{11}$. Here $t_2$ should be 0 mod (5) and (11), so $t_2 = \alpha \cdot 5 \cdot 11$. We want $t_2 \equiv 1 \text{ mod } 2$, so $\alpha = 1$ suffices. Similarly, one can use
\[ t_7 = 2 \cdot 11 \cdot 1 \quad \text{and} \quad t_{11} = 2 \cdot 7 \cdot 4. \]
This $t_{11}$ arises from $2 \cdot 7 = 14 \equiv 3 \text{ mod } 11$ and $3 \cdot 4 = 12 \equiv 1 \text{ mod } 11$.

The final answer is
\[ c = 1 \cdot 7 \cdot 11 + 3 \cdot 2 \cdot 11 + 5 \cdot 2 \cdot 7 \cdot 4 = 423 \]


**Euclidean rings**

Suppose $R$ is a commutative ring. Let $\mathbb{Z}_{\geq 0}$ be the non-negative integers.

**Def:** A function $N : R \to \mathbb{Z}_{\geq 0}$ is a norm if $N(0)$ and $N(r) > 0$ if $r \neq 0$.

**Def:** $R$ is a **Euclidean ring** if $R$ is an integral domain, and there is a norm $N$ on $R$ with the following property. For each $a, b \in R$ such that $b \neq 0$, there are $q, r \in R$ such that

1. $a = qb + r$, and

2. Either $r = 0$ or $N(r) < N(b)$.

One then says $N$ is a Euclidean norm.

**Example:** If $R = \mathbb{Z}$, the usual absolute value $N(a) = |a|$ is a Euclidean norm.
Euclidean rings are of interest for this reason:

**Theorem:** Every Euclidean ring $R$ is a P.I.D., i.e. all of its ideals are principal.

**Proof:** Suppose $A$ is an ideal of the Euclidean ring $R$, and that $N$ is a Euclidean norm on $R$. If $A = \{0\}$ this is certainly a principal ideal, so suppose $A \neq \{0\}$.

Since $N$ takes values in $\mathbb{Z}_{\geq 0}$, and every non-empty subset of $\mathbb{Z}_{\geq 0}$ has a unique smallest element, there is an element $0 \neq b \in A$ such that

$$N(b) \leq N(r)$$

for all $0 \neq r \in A$. We claim that $A = Rb$.

Suppose $a$ is any element of $A$. By the Euclidean property of $N$, we have

$$a = qb + r$$

for some $q, r \in R$ with $r = 0$ or $N(r) < N(b)$. However, $r = a - qb \in A$, so the minimality of $N(b)$ shows $r = 0$ and $a = qb \in Rb$. 


**Example:** Suppose $F$ is a field and $R = F[x]$. Define $N : F[x] \to \mathbb{Z}_{\geq 0}$ by $N(0) = 0$ and $N(f(x)) = \deg(f(x))$ if $0 \neq f(x) \in R$. Then the usual division algorithm for polynomials shows $N$ is a Euclidean norm. One uses the algorithm to find a polynomial $q$ so the remainder $r = a - qb$ is either 0 or has smaller degree than the polynomial $b \neq 0$.

**Example:** Suppose $i = \sqrt{-1} \in \mathbb{C}$, and that $R$ is the quadratic integer ring $\mathbb{Z}[i]$. We can then picture the elements of $R$ as the integral lattice points in the complex plane:
Let’s show that \( N : R = \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0} \) defined by
\[
N(r) = |c + di|^2 = c^2 + d^2.
\]
is a Euclidean norm.

Suppose
\[
a = u + vi \quad \text{and} \quad b = w + si
\]
are two elements of \( R \) with \( b \neq 0 \). We have to produce \( q, r \in R \) such that
\[
a = qb + r
\]
and \( r = 0 \) or \( N(r) < N(b) \).

Rewrite this equation as
\[
\frac{a}{b} = q + \frac{r}{b}
\]
in \( \mathbb{C} \).
We let $q = m + ni$ be one of the lattice points in $R$ of minimal distance from the complex number $\frac{a}{b}$.

The distance between $q$ and $\frac{a}{b}$ is bounded by $\sqrt{2}/2$. So

$$\left| \frac{r}{b} \right| = \left| \frac{a}{b} - q \right| \leq \sqrt{2}/2$$

Squaring this gives

$$N(r)^2/N(b)^2 = \left| \frac{r}{b} \right|^2 \leq \frac{1}{2}$$

which proves $N(r) < N(b)$ in all cases.

(Note that if $N(r) < 1$, then $r = 0$.)
**Example:** Suppose $F$ is a field. A discrete valuation on $F$ is a function $v : F^* - \{0\} \to \mathbb{Z}$ such that:

1. $v$ is surjective.

2. $v(ab) = v(a) + v(b)$.

3. $v(a + b) \geq \min(v(a), v(b))$.

These properties imply that the set

$$R = \{0\} \cup \{r \in R : v(r) \geq 0\}$$

is a ring, which we will call the valuation ring of $v$. (For example, $v(1 \cdot 1) = v(1) + v(1)$ forces $v(1) = 0$; then $v(-1 \cdot -1) = v(1) = 0$ means $v(-1) = 0$. Now from (2) and (3) we see $R$ is closed under multiplication and subtraction.)

In general, an integral domain will be called a discrete valuation ring if it is the valuation ring of a discrete valuation of its quotient field.
**Theorem:** Discrete valuation rings (D.V.R.’s) are Euclidean.

**Proof:** We define \( N : R \to \mathbb{Z}_{\geq 0} \) by \( N(0) = 0 \) and \( N(r) = v(r) \) if \( 0 \neq r \in R \).

To show the Euclidean property, suppose \( a, b \in R \) and \( 0 \neq b \). We have to find \( q, r \in R \) with

\[
a = qb + r
\]

and \( r = 0 \) or \( N(r) < N(b) \).

If \( a = 0 \) then \( q = r = 0 \) suffices, so suppose \( a \neq 0 \).

If \( v(a) \geq v(b) \) then \( v(a/b) = v(a) - v(b) \geq 0 \) so \( q = a/b \in R \) and we can let \( r = 0 \).

Suppose finally that \( v(a) < v(b) \). This case is easy: let \( q = 0 \) and \( r = a \).
**Example:** Suppose $p$ is a rational prime. There is a discrete valuation

$$v_p : \mathbb{Q}^* \rightarrow \mathbb{Z}$$

defined by letting

$$v_p\left(\frac{a}{b}\right) = \text{ord}_p(a) - \text{ord}_p(b)$$

for all non-zero integers $a, b$, where $\text{ord}_p(a)$ is the exponent of the highest power of $p$ which divides $a$. The valuation ring of $v_p$ is just the localization

$$\mathcal{O}_p = \left\{ \frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b \right\}$$

It will be a homework problem on the next homework assignment to check that every discrete valuation of $\mathbb{Q}$ has the form $v_p$ for some prime $p$. 

13
**Example:** Suppose $F = C(t)$ is the rational function field in one variable. If $\alpha \in C$, we can define a discrete valuation

$$v_\alpha : C(t)^* \to \mathbb{Z}$$

by

$$v_\alpha(f(x)) = n$$

if

$$f(x) = (x - \alpha)^n \cdot \frac{s(x)}{t(x)} \quad \text{with} \quad s(\alpha) \neq 0 \neq t(\alpha).$$

The discrete valuation ring of $v_\alpha$ is the localization

$$C[x]_{(x-\alpha)} = \left\{ \frac{h(x)}{g(x)} : h(x), g(x) \in C[x], g(\alpha) \neq 0 \right\}$$

and all the discrete valuations of $C(t)$ have the form $v_\alpha$ for some $\alpha \in C$. 
**Example:** If $p$ is a prime, the $p$-adic integers $\mathbb{Z}_p$ form the valuation ring of the discrete valuation

$$v_p : \mathbb{Q}_p^* \rightarrow \mathbb{Z}$$

defined in the following way.

Let $v_p(r) = n$ if $rp^{-n}$ is a unit of $\mathbb{Z}_p$.

This is equivalent to saying that $r$ can be represented in the form

$$r = p^n \sum_{i=0}^{\infty} a_ip^i$$

with $a_i \in \{0, \ldots, p-1\}$ for all $i$ and $a_0 \neq 0$. 