CRT for PIDs

R PID, $f, g \in R$, $(f)+(g)=(1)$

Claim: $\dfrac{R}{(fg)} \cong \dfrac{R}{(f)} \times \dfrac{R}{(g)}$

$\psi : R \longrightarrow \dfrac{R}{(f)} \times \dfrac{R}{(g)}$

$\psi(h) = (h+(f), h+(g))$ ring hom.

Surj: take $h_1, h_2 \in R$, want $u \in R$ with

$$u \equiv h_1 \mod (f)$$
$$u \equiv h_2 \mod (g)$$

Bezout: $1 = cf + dg$ so $cf \equiv 1 \mod (g)$, $dg \equiv 1 \mod (f)$

$u = dgh_1 + cfh_2$

$u \equiv dgh_1 \equiv h_1 \mod f$

$u \equiv cfh_2 \equiv h_2 \mod g$

Ker: $\psi : R \longrightarrow \dfrac{R}{(f)} \times \dfrac{R}{(g)}$

$\psi(u) = (u+(f), u+(g))$

$\psi(u) = (0+(f), 0+(g))$ iff $u \in (f) \cap (g)$

But: $\gcd(f,g)=1$ si $(f) \cap (g) = (fg)$.

Ex $f = x^2+1 \in \mathbb{Q}[x]$, $g = x^2+2 \in \mathbb{Q}[x]$

$U = \dfrac{\mathbb{Q}[x]}{(fg)}$, $a = \bar{x} = x + (fg) \in R$

$fg = (x^2+1)(x^2+2) = x^4 + 3x^2 + 2$

What is a^8 (expressed in basis $1, a, a^2, a^3$) ?

Can calculate $a^4 = -3a^2 + 2$

$a^5 = -3a^3 + 2a$

$a^6 = -3a^4 + 2a^2 = -3(-3a^2+2) + 2a^2$

$= -7a^2 - 6$

et cetera,

INEFFICIENT

$S = \frac{\mathbb{Q}[x]}{(f)} = \mathbb{Q}(b)$, $b = \bar{x}$, $b^2 = -1$, $T = \frac{\mathbb{Q}[x]}{(g)} = \mathbb{Q}(c)$, $c = \bar{x}$,

$c^2 = -2$

another c, sorry

$b^8 = 1$ in S

$$b^8 : (b^2-1) = b^6 + b^4 + b^2 + 1$$

$b^8 - b^6$

b^6

$b^6 - b^4$

b^4

$b^4 - b^2$

b^2

$b^2 - 1$

1

$c^8 = 16$ in T

$$c^8 : (c^2-2) = c^6 + 2c^4 + 4c^2 + 8$$

$c^8 - 2c^6$

$2c^6$

$2c^6 - 4c^4$

$4c^4$

$4c^4 - 8c^2$

$8c^2$

$8c^2 - 16$

16

$a^8 \equiv 1 \mod x^2+1$ $\quad | \quad 1 = \underset{c}{-1}\underset{f}{(x^2+1)} + \underset{d}{1}\underset{g}{(x^2+2)}$

$a^8 \equiv \underset{h_2}{16} \mod x^2+2$

$u = cfh_2 + dgh_1$

$\equiv -1 \cdot (x^2+1) \cdot 16 + 1 \cdot (x^2+2) \cdot 1 \equiv -15x^2 - 14$

Sa: $a^8 \equiv -15a^2 - 14$: $\frac{\mathbb{Q}[x]}{(x^2+1)(x^2+2)} = \mathbb{Q}(a)$

$$\frac{R}{(fg)} \overset{\tilde{\Psi}}{\cong} \frac{R}{(f)} \times \frac{R}{(g)}$$ as before

$u \in R$, look for inverse mod (fg), call v if exists

$uv \equiv 1 \mod (fg)$

Then: $\Psi(uv) = (uv + (f), uv + (g)) = (1+(f), 1+(g))$

So $(u+(f))(v+(f)) = uv + (f) = 1 + (f)$

Conversely: if $uv_1 \equiv 1 \mod (f)$
$uv_2 \equiv 1 \mod (g)$

then find v s.t $v \equiv v_1 \mod f$
$v \equiv v_2 \mod g$

i.e $v = dgv_1 + cfv_2$

Then $uv \equiv 1 \mod (f)$
$uv \equiv 1 \mod (g)$

so $uv \equiv 1 \mod (fg)$

Ex $R = \mathbb{Q}[x]$, $f = x^2+1$, $g = x^2+2$

$c = -1$, $d = 1$

$u = x^3$, is there an inverse?

mod x^2+1: $\gcd(x^2+1, x^3) = 1$

$1 = (-x^2+1)(x^2+1) + x \cdot x^3$

$1 \equiv x \cdot x^3 \mod (x^2+1)$

mod x^2+2:

$1 = \left(-\frac{1}{4}x^2+\frac{1}{2}\right)(x^2+2) + \frac{1}{4}x x^3$

$1 \equiv \frac{1}{4} x x^3 \mod (x^2+2)$

$v \equiv x \mod x^2+1$

$v \equiv \frac{1}{4}x \mod x^2+2$

$v = dg v_1 + cf v_2 = 1 \cdot (x^2+2) \cdot x + (-1) \cdot (x^2+1) \cdot \frac{1}{4} x$

$= \frac{3}{4}x^3 + \frac{7}{4}x$

$x^3 v = \frac{3}{4}x^6 + \frac{7}{4}x^4 \equiv 1 \mod (fg)$