CS250:	**Draft Crib Sheet for Final**	**F2016**

Tarski's Definition of Truth

$$
\begin{array}{llll}
G & \models & t_1 = t_2 & \text{iff} \quad t_1^G = t_2^G \\
G & \models & P(t_1,\ldots,t_a) & \text{iff} \quad (t_1^G,\ldots,t_a^G) \in P^G \\
G & \models & \sim\alpha & \text{iff} \quad G \not\models \alpha \\
G & \models & \alpha \wedge \beta & \text{iff} \quad G \models \alpha \quad \textbf{and} \quad G \models \beta \\
G & \models & \alpha \vee \beta & \text{iff} \quad G \models \alpha \quad \textbf{or} \quad G \models \beta \\
G & \models & \forall x(\alpha) & \text{iff} \quad \textbf{for all } a \in |G| \quad G[a/x] \models \alpha \\
G & \models & \exists x(\alpha) & \text{iff} \quad \textbf{exists } a \in |G| \quad G[a/x] \models \alpha
\end{array}
$$

Logical Equivalences and Abbreviatons

$$
\begin{array}{rcl}
p \to q & \equiv & \sim p \vee q \\
\sim(p \wedge q) & \equiv & \sim p \vee \sim q \\
\sim\forall x\, \varphi & \equiv & \exists x\ \sim\varphi \\
\sim(p \vee q) & \equiv & \sim p \wedge \sim q \\
\sim\exists x\, \varphi & \equiv & \forall x\ \sim\varphi \\
p \text{ only if } q & \equiv & p \to q \\
p \text{ if } q & \equiv & q \to p \\
p \text{ iff } q & \equiv & p \leftrightarrow q \\
p \text{ is necessary for } q & \equiv & q \to p \\
p \text{ is sufficient for } q & \equiv & p \to q \\
p \text{ unless } q & \equiv & \sim q \ \to\ p \\
t_1 \neq t_2 & \equiv & \sim(t_1 = t_2) \\
(\forall x\,.\,\alpha)\beta & \equiv & \forall x(\alpha \to \beta) \\
(\exists x\,.\,\alpha)\beta & \equiv & \exists x(\alpha \wedge \beta) \\
\exists! x(\alpha(x)) & \equiv & \exists x \forall y(\alpha(x) \wedge (\alpha(y) \to y = x)) \\
x|y & \equiv & \exists z\ (x \cdot z = y) \\
a \equiv b \pmod{m} & \equiv & m|(a-b) \\
\text{prime}(x) & \equiv & 1 < x \wedge \forall y\ (1 < y \wedge y|x \to y = x)
\end{array}
$$

Natural Deduction Rules

Proviso for $\forall$-i and $\exists$-e: x_0 is a "new" variable, i.e., it does not appear in φ, ψ, or Γ.

	introduction	elimination
$\wedge$	$\dfrac{\alpha \quad \beta}{\alpha \wedge \beta}$	$\dfrac{\alpha \wedge \beta}{\alpha}$ $\quad$ $\dfrac{\alpha \wedge \beta}{\beta}$
$\vee$	$\dfrac{\alpha}{\alpha \vee \beta}$ $\quad$ $\dfrac{\beta}{\alpha \vee \beta}$	$\dfrac{\alpha \vee \beta \quad \alpha \vdash \psi \quad \beta \vdash \psi}{\psi}$
$\to$	$\dfrac{\alpha \vdash \beta}{\alpha \to \beta}$	$\dfrac{\alpha \to \beta \quad \alpha}{\beta}$ $\quad$ $\dfrac{\alpha \to \beta \quad \sim\beta}{\sim\alpha}$
$\mathbf{F}$	$\dfrac{\alpha \quad \sim\alpha}{\mathbf{F}}$	$\dfrac{\alpha \vdash \mathbf{F}}{\sim\alpha}$ $\quad$ $\dfrac{\sim\alpha \vdash \mathbf{F}}{\alpha}$
$\sim\sim$	$\dfrac{\alpha}{\sim\sim\alpha}$	$\dfrac{\sim\sim\alpha}{\alpha}$
$=$	$\overline{t = t}$	$\dfrac{t_1 = t_2 \quad \varphi[t_1/x]}{\varphi[t_2/x]}$
$\forall$	$\dfrac{\Gamma \vdash \varphi[x_0/x]}{\Gamma \vdash \forall x\, \varphi}$	$\dfrac{\forall x\, \varphi}{\varphi[t/x]}$
$\exists$	$\dfrac{\varphi[t/x]}{\exists x\, \varphi}$	$\dfrac{\Gamma \vdash \exists x\, \varphi \quad \Gamma, \varphi[x_0/x] \vdash \psi}{\Gamma \vdash \psi}$

Truth Game: literal: **D** wins iff $W \models \varphi$

$\wedge, \forall$: **G** chooses $\quad$ $\vee, \exists$: **D** chooses

Euclid's Algorithm $\gcd(a,b) = ax + by$.

If $\gcd(a,b) = 1$ then $a^{-1} \bmod b = (x\%b)$.

$$\varphi(m) = |\mathbf{Z}_m^*| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a,m) = 1\right\}\right|$$

$$\varphi(p_1^{a_1} \cdots p_k^{a_k}) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - 1})$$

$$a|(bc) \wedge \gcd(a,b) = 1 \ \to\ a|c$$

RSA: publish, $n = p \cdot q, e$, keep secret:
$p, q, \varphi(n), d$ where $d = e^{-1} \pmod{\varphi(n)}$.

CRT: $\forall a, b > 1\, (\gcd(a,b) = 1 \ \to\ \forall x \in \mathbf{Z}/a\mathbf{Z}\ \forall y \in \mathbf{Z}/b\mathbf{Z}\ \exists! z \in \mathbf{Z}/ab\mathbf{Z}\ (z \equiv x \pmod{a}\ \wedge\ z \equiv y \pmod{b}))$

Proof: $\quad z \stackrel{\text{def}}{=} f(x,y) \stackrel{\text{def}}{=} \big(x \cdot b \cdot (b^{-1} \bmod a) + y \cdot a \cdot (a^{-1} \bmod b)\big)\ \%\ ab$