APPENDIX G
Proof of the Digital Signature Algorithm

William Stallings

Supplement to
Cryptography and Network Security, Fourth Edition
Prentice Hall 2006
ISBN: 0-13-187316-4
http://williamstallings.com/Crypto/Crypto4e.html

The purpose of this appendix is to provide a proof that in the DSA signature verification we have $v = r$ if the signature is valid. The following proof is based on that which appears in the FIPS standard, but it includes additional details to make the derivation clearer.

LEMMA 1. For any integer t, **if** $g = h^{(p-1)/q} \bmod p$

then $g^t \bmod p = g^{t \bmod q} \bmod p$

Proof: By Fermat's theorem (Chapter 8), because h is relatively prime to p, we have $H^{p-1} \bmod p = 1$. Hence, for any nonnegative integer n,

$$
\begin{aligned}
g^{nq} \bmod p &= \left(h^{(p-1)/q} \bmod p\right)^{nq} \bmod p \\
&= h^{((p-1)/q)nq} \bmod p && \text{by the rules of modular arithmetic} \\
&= h^{(p-1)n} \bmod p \\
&= \left(\left(h^{(p-1)} \bmod p\right)^{n}\right) \bmod p && \text{by the rules of modular arithmetic} \\
&= 1^{n} \bmod p = 1
\end{aligned}
$$

So, for nonnegative integers n and z, we have

$$
\begin{aligned}
g^{nq+z} \bmod p &= (g^{nq}\, g^{z}) \bmod p \\
&= \left(\left(g^{nq} \bmod p\right)\left(g^{z} \bmod p\right)\right) \bmod p \\
&= g^{z} \bmod p
\end{aligned}
$$

Any nonnegative integer t can be represented uniquely as $t = nq + z$, where n and z are nonnegative integers and $0 < z < q$. So $z = t \bmod q$. The result follows. **QED**.

LEMMA 2. For nonnegative integers a and b: $g^{(a \bmod q\, +\, b \bmod q)} \bmod p = g^{(a+b) \bmod q} \bmod p$

Proof: By Lemma 1, we have

$$\begin{aligned} g^{(a \bmod q\, +\, b \bmod q)} \bmod p &= g^{(a \bmod q\, +\, b \bmod q) \bmod q} \bmod p \\ &= g^{(a\, +\, b) \bmod q} \bmod p \end{aligned}$$

QED.

LEMMA 3. $y^{(rw) \bmod q} \bmod p \;=\; g^{(xrw) \bmod q} \bmod p$

Proof: By definition (Figure 13.2), $y = g^x \bmod p$. Then:

$$\begin{aligned} y^{(rw) \bmod q} \bmod p &= (g^x \bmod p)^{(rw) \bmod q} \bmod p \\ &= g^{x\,((rw) \bmod q)} \bmod p && \text{by the rules of modular arithmetic} \\ &= g^{(x\,((rw) \bmod q)) \bmod q} \bmod p && \text{by Lemma 1} \\ &= g^{(xrw) \bmod q} \bmod p \end{aligned}$$

QED.

LEMMA 4. $((\mathrm{H(M)} + xr)w) \bmod q = k$

Proof: By definition (Figure 13.2), $s = \left(k^{-1}\left(\mathrm{H}\left(\mathrm{M}\right) + xr\right)\right) \bmod q$. Also, because q is prime, any nonnegative integer less than q has a multiplicative inverse (Chapter 8). So $(k\,k^{-1}) \bmod q = 1$. Then:

$$\begin{aligned}(ks) \bmod q &= \left(k\left(\left(k^{-1}(\mathrm{H}(\mathrm{M}) + xr)\right) \bmod q\right)\right) \bmod q \\ &= \left(\left(k\left(k^{-1}(\mathrm{H}(\mathrm{M}) + xr)\right)\right)\right) \bmod q \\ &= \left(\left(\left(kk^{-1}\right) \bmod q\right)\left((\mathrm{H}(\mathrm{M}) + xr) \bmod q\right)\right) \bmod q \\ &= \left((\mathrm{H}(\mathrm{M}) + xr)\right) \bmod q\end{aligned}$$

By definition, $w = s^{-1} \bmod q$ and therefore $(ws) \bmod q = 1$. Therefore,

$$\begin{aligned}((\mathrm{H}(\mathrm{M}) + xr)w) \bmod q &= (((\mathrm{H}(\mathrm{M}) + xr) \bmod q)\ (w \bmod q)) \bmod q \\ &= (((ks) \bmod q)\ (w \bmod q)) \bmod q \\ &= (kws) \bmod q \\ &= ((k \bmod q)\ ((ws) \bmod q)) \bmod q \\ &= k \bmod q\end{aligned}$$

Because $0 < k < q$, we have $k \bmod q = k$. **QED.**

THEOREM: Using the definitions of Figure 13.2, $v = r$.

$$\begin{aligned}v &= \left(\left(g^{u1}y^{u2}\right) \bmod p\right) \bmod q && \text{by definition} \\ &= \left(\left(g^{(\mathrm{H}(\mathrm{M})w) \bmod q}\, y^{(\mathrm{r}w) \bmod q}\right) \bmod p\right) \bmod q \\ &= \left(\left(g^{(\mathrm{H}(\mathrm{M})w) \bmod q}\, g^{(\mathrm{xr}w) \bmod q}\right) \bmod p\right) \bmod q && \text{by Lemma 3} \\ &= \left(\left(g^{(\mathrm{H}(\mathrm{M})w) \bmod q + (\mathrm{xr}w) \bmod q}\right) \bmod p\right) \bmod q\end{aligned}$$

$$\begin{aligned}
&= \left(\left(g^{\left(\mathrm{H}(\mathrm{M})w+\mathrm{xr}w\right)\bmod q}\right)\bmod p\right)\bmod q && \text{by Lemma 2}\\
&= \left(\left(g^{\left(\left(\mathrm{H}(\mathrm{M})+\mathrm{xr}\right)w\right)\bmod q}\right)\bmod p\right)\bmod q && \\
&= \left(gk \bmod p\right)\bmod q && \text{by Lemma 4}\\
&= r && \text{by definition}
\end{aligned}$$

QED.