# Proof Sketch for the Montgomery Multiplication

| | |
|---|---|
| `Definition montgomery k alpha` | |
| `x y z m j i X Y M Z` | |
| `one zero quot C t s :=` | $\{(z_0 \cdots z_{k-1}) = 0 \wedge m_0 \cdot \alpha \equiv -1[\beta] \wedge \mathtt{acx} \Vert \mathtt{hi} \Vert \mathtt{lo} = 0\}$ |
| `addiu one zero one16;` | $\{\ldots\}$ |
| `addiu C zero zero16;` | $\{\ldots\}$ |
| `addiu i zero zero16;` | $\{\ldots\}$ |
| `while_ne i k (` | $\boxed{\{\beta^i (z_0 \cdots z_{k-1} C)_\beta = (x_0 \cdots x_{i-1})_\beta \cdot y + K_i \cdot m\}}$ |
| `lwxs X i x; lw Y zero16 y; lw Z zero16 z;` | $\{\ldots\}$ |
| `multu X Y;` | $\{\mathtt{acx} = 0\}$ |
| `lw M zero16 m;` | $\{\ldots\}$ |
| `maddu Z one;` | $\{\ldots\}$ |
| `mflo t; mfhi s;` | $\{\ s \Vert t = (z_0 + x_i \cdot y_0)\%64 = z_0 + x_i \cdot y_0\ \}$ |
| `multu t alpha;` | $\{\mathtt{acx} = 0\}$ |
| `addiu j zero one16;` | $\{\ldots\}$ |
| `mflo quot;` | $\{q_i = (((z_0 + x_i \cdot y_0)\%32)\alpha)\%32\}$ |
| `mthi s; mtlo t;` | $\{\ldots\}$ |
| `maddu quot M;` | $\{\mathtt{lo} = 0\}$ |
| `mflhxu Z;` | $\{\mathtt{hi} \Vert \mathtt{lo} = (z_0 + x_i \cdot y_0 + q_i \cdot m_0)/\beta \wedge \mathtt{acx} = 0\}$ |
| `addiu t z zero16;` | $\left\{ \begin{array}{l} \beta^i (z_0 \cdots z_{k-1} C)_\beta = (x_0 \cdots x_{i-1})_\beta \cdot y + K_i \cdot m \wedge \\ \beta(\mathtt{hi} \Vert \mathtt{lo}) = z_0 + x_i \cdot y_0 + q_i \cdot m_0 \end{array} \right\}$ |
| `while_ne j k (` | $\boxed{\left\{ \begin{array}{l} \beta^{i+1}((z_{0 \cdots k-1 \setminus \{j-1\}} C)_\beta) + (\mathtt{hi} \Vert \mathtt{lo})\beta^{i+j} = \\ (x_{0 \cdots i-1})_\beta \cdot y + K_i \cdot m + \\ (y_{0 \cdots j-1})_\beta \cdot x_i \cdot \beta^i + (m_{0 \cdots j-1})_\beta \cdot q_i \cdot \beta^i \wedge \\ \mathtt{acx} = 0 \wedge \mathtt{acx} \Vert \mathtt{hi} \Vert \mathtt{lo} < 2\beta - 1 \end{array} \right\}}$ |
| `  lwxs Y j y; lwxs Z j z;` | $\{\ldots\}$ |
| `  maddu X Y;` | $\{\ldots\}$ |
| `  lwxs M j m;` | $\{\ldots\}$ |
| `  maddu Z one;` | $\{\ldots\}$ |
| `  maddu quot M;` | $\{\ldots\}$ |
| `  addiu j j one16;` | $\{\ldots\}$ |
| `  mflhxu Z;` | $\left\{ \begin{array}{l} Z = (z_j + x_i \cdot y_j + q_i \cdot m_j)\%32 \wedge \\ \mathtt{hi} \Vert \mathtt{lo} = (x_k + x_i \cdot y_j + q_i \cdot m_j)/\beta \end{array} \right\}$ |
| `  addiu t t four16;` | $\{\ldots\}$ |
| `  sw Z m4_16bit t` | $\{\ldots\}$ |
| `); (* loop exit *)` | $\left\{ \begin{array}{l} \beta^{i+1}((z_{0 \cdots k-2} C)_\beta) + (\mathtt{hi} \Vert \mathtt{lo})\beta^{i+k} = \\ (x_{0 \cdots i-1})_\beta \cdot y + K_i \cdot m + \\ (y_{0 \cdots k-1})_\beta \cdot x_i \cdot \beta^i + (m_{0 \cdots k-1})_\beta \cdot q_i \cdot \beta^i \wedge \\ \mathtt{acx} = 0 \end{array} \right\}$ |
| `maddu C one;` | $\left\{ \begin{array}{l} \beta^{i+1}(z_{0 \cdots k-2})_\beta + (\mathtt{hi} \Vert \mathtt{lo})\beta^{k+i} = \ldots \wedge \\ \mathtt{acx} = 0 \end{array} \right\}$ |
| `mflhxu Z;` | $\left\{ \begin{array}{l} \beta^{i+1}(z_{0 \cdots k-2})_\beta + Z \cdot \beta^{k+i} + \mathtt{lo} \cdot \beta^{k+i+1} = \ldots \wedge \\ \mathtt{hi} = 0 \wedge \mathtt{acx} = 0 \end{array} \right\}$ |
| `addiu i i one16;` | $\{\ldots\}$ |
| `sw Z zero16 t;` | $\left\{ \begin{array}{l} \beta^i (z_{0 \cdots k-1})_\beta + \mathtt{lo} \cdot \beta^{k+i} = \\ (x_{0 \cdots i-2})_\beta \cdot y + K_i \cdot m + y \cdot x_{i-1} \cdot \beta^{i-1} + m \cdot q_i \cdot \beta^{i-1} \end{array} \right\}$ |
| `mflhxu C` | $\left\{ \begin{array}{l} \beta^i (z_{0 \cdots k-1})_\beta + C \cdot \beta^{k+i} = \\ (x_{0 \cdots i-1})_\beta \cdot y + (K_i + q_i \cdot \beta^{i-1}) \cdot m \wedge \\ \mathtt{lo} = 0 \end{array} \right\}$ |
| `). (* loop exit *)` | $\{\beta^k (z_0 \cdots z_{k-1} C)_\beta = x \cdot y + K_{i+1} \cdot m\}$ |